CHAPITRE I IDÉAUX D'UN CORPS QUADRATIQUE

CHAPITRE I

IDÉAUX D'UN CORPS QUADRATIQUE

1. Construction d'un corps quadratique.

Un *corps quadratique est caractérisé par un nombre entier*, d, différent de 0 et de $+1$, sans facteur carré; ou, plus précisément, *par le trinome du second degré normé* (de premier coefficient égal à $+1$), *appelé* **polynôme fondamental** *du corps*:

$$F(x) = x^2 - Sx + N,$$

dont les coefficients sont, suivant la divisibilité de $d-1$ par 4:

$d-1$ div. par 4:

$$S = -1, \quad N = (1-d):4, \quad 4F(x) = (2x+1)^2 - d;$$

$d-1$ non div. par 4:

$$S = 0, \quad N = -d, \quad F(x) = x^2 - d.$$

Ce trinôme peut être mis sous la forme (commune aux deux cas):

$$4F(x) = (2x-S)^2 - D; \quad D = S^2 - 4N = \begin{cases} d \\ 4d \end{cases};$$

D est appelé le **discriminant** du corps.

Le trinôme est *irréductible* —ou sans zéro rationnel—, puisque D n'est pas carré parfait (le cas $d = +1$ —ou $D = +4$— étant exclus).

Si d —donc aussi D— est positif, le trinôme a deux zéros *réels*, (non rationnels), on dit que le corps est *réel*; si d —donc D— est négatif, le trinôme a deux zéros *complexes*, le corps est dit *imaginaire*.

On peut donner du corps diverses *constructions* équivalentes:

Le **corps quadratique**, caractérisé par le polynôme fondamental $F(x)$, désigné par $\mathbf{R}(\theta)$, *peut être obtenu en « adjoignant »*, par addition, soustraction et multiplication, *au corps* **R**, des nombres rationnels, *un symbole* —ou *générateur*—, désigné par θ, *qui se comporte comme un zéro de* $F(x)$.

On peut entendre par là que ce corps $\mathbf{R}(\theta)$ est l'ensemble des valeurs $f(\theta)$, des expressions entières —ou polynômes— $f(x)$, à coefficients rationnels, pour la valeur θ, de l'indéterminée x. Toutefois chacune d'elles est (considérée comme) *égale* à la valeur $r+s\theta$, du binôme:

$$r+sx = f(x)—F(x)\times q(x),$$

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

Il est équivalent de dire qu'un *élément* de $\mathbf{R}(\theta)$ est l'*ensemble des expressions* (considérées comme) *égales entre elles*:

$r+s\theta+F(\theta)\times q(\theta)$; $q(x)$ polynôme à coefficients dans **R**; (la valeur $F(\theta)$ se comportant comme un *élément nul*).

On se borne, ordinairement, à utiliser les expressions linéaires $r+s\theta$, les autres servant seulement à définir, [ou à justifier], leur calcul. Deux éléments sont égaux, si et seulement si leurs expressions linéaires ont des *coefficients* (rationnels) égaux:

$$(r+s\theta) = (r'+s'\theta) \quad \Leftrightarrow \quad \{r = r' \quad \text{et} \quad s = s'\}.$$

Les règles explicites des *opérations internes* (*addition*, de signe $+$, *multiplication*, de signe $\times$) se déduisent du « comportement » de θ ou de la règle du reste (qui revient à remplacer θ^2 par $S\theta—N$):

$$(r+s\theta)+(r'+s'\theta) = (r+r')+(s+s')\theta;$$
$$(r+s\theta)\times(r'+s'\theta) = (rr'—Nss')+(rs'+sr'+Sss')\theta.$$

Ces règles (ou le calcul des expressions entières et la règle du reste), montrent que ces deux opérations ont les qualités usuelles: elles sont *associatives*, *commutatives* et la multiplication est *distributive* relativement à l'addition.

Les binômes $0+0\theta$ (en abrégé 0) et $1+0\theta$ (en abrégé 1), sont les éléments *nul* (neutre pour l'addition) et *unité* (neutre pour la multiplication). Chaque élément $r+s\theta$ a un *opposé* déterminé:

$$(-r)+(-s)\theta = (-1+0\theta)\times(r+s\theta), \text{ en abrégé } -(r+s\theta).$$

La somme de deux opposés est égale à l'élément nul, la *soustraction* (opération inverse de l'addition) est possible et déterminée: soustraire un élément est équivalent à additionner son opposé [1]).

On peut aussi considérer que *le corps quadratique* $\mathbf{R}(\theta)$ *est un ensemble d'éléments*, désignés par les lettres grecques $\rho,\alpha,\beta,\ldots$, qui sont des *formes* (linéaires) de deux symboles: 1 (*unité*) et θ *générateur*:

$$\rho = r\times(1)+s\times(\theta), \quad \text{en abrégé } r+s\theta;$$

dont les *variables*, ou *multiplicateurs*, des symboles 1 et θ, désignées par des lettres latines: $r,s,a,b,\ldots$ sont des *nombres rationnels.*

Les opérations (addition, soustraction, multiplication), entre ces éléments sont les mêmes qu'entre les formes; toutefois la multiplication, distributive relativement à l'addition, est définie par la table de multiplication (commutative et associative) des symboles:

$$(1)\times(1) = (1); \quad (1)\times(\theta) = (\theta)\times(1) = (\theta);$$
$$(\theta)\times(\theta) = -N+S\theta.$$

Les éléments, pour lesquels le multiplicateur de θ est nul:

$$r\times(1)+0\times\theta, \quad \text{en abrégé } r,$$

qui comprennent les éléments nul, et unité, sont appelés les *éléments rationnels* du corps; ils se calculent entre eux (égalité et opérations) comme les nombres rationnels (éléments du corps $\mathbf{R}$).

De la construction adoptée pour $\mathbf{R}(\theta)$, il résulte que, dans cet ensemble, *le polynôme fondamental* $F(x)$ *est décomposable en* —ou égal à— *un produit de deux binômes linéaires normés*:

$$F(x) = (x-\theta)\times(x-\theta'); \quad \theta' = S\times(1)+(-1)\times\theta, \quad \text{ou} \quad S-\theta.$$

On peut dire que, dans $\mathbf{R}(\theta)$, $F(x)$ a deux *zéros* θ *et* θ', tels que:

[1]) On reconnaît, dans ce calcul, une construction analogue à celle des *nombres complexes*, dans le corps des nombres réels, par les congruences de Cauchy. Plus généralement, on peut dire que $\mathbf{R}(\theta)$ est isomorphe à l'anneau quotient $\mathbf{R}(x)|F(x)$; [$\mathbf{R}(x)$ anneau des polynômes à coefficients rationnels; $F(x)$ polynôme fondamental].

$$\theta+\theta' = S; \quad \theta\times\theta' = N; \quad (\theta—\theta')^2 = S^2—4N = D.$$

Le corps $\mathbf{R}(\theta)$ peut être construit aussi avec les deux symboles: l'unité 1 et le générateur θ', moyennant la correspondance (biunivoque) suivante des multiplicateurs:

$$r+s\theta = r'+s'\theta' \Leftrightarrow r' = r+sS \quad \text{et} \quad s' = —s.$$

1. 2. *Inverses et division.*

L'irréductibilité de $F(x)$ —ou l'inexistence de zéro rationnel— permet d'affirmer que: *tout élément* $\rho = r+s\theta$, *non nul*, de $\mathbf{R}(\theta)$, *a un et un seul* **inverse**, c'est-à-dire qu'*il existe un élément* (unique), désigné (suivant la notation habituelle) par ρ^{-1}, *tel que le produit* $\rho\times\rho^{-1}$ *soit égal à l'élément unité* $+1$.

Pour obtenir cet inverse, on peut calculer le produit:

$$(r+s\theta)\times(r+s\theta') = r^2+Srs+Ns^2 = s^2\times F(—r:s) = q;$$

c'est un *élément rationnel* du corps, qui n'est pas nul (r et s ne l'étant pas simultanément), puisque $F(x)$ n'a pas de zéro rationnel. Le quotient de $r+s\theta'$ par ce nombre rationnel q:

$$\rho^{-1} = \frac{r}{q}+\frac{s}{q}\theta', \quad \text{ou} \quad \frac{r+Ss}{q}—\frac{s}{q}\theta;$$

est l'inverse cherché puisque $\rho\times\rho^{-1} = q:q = +1$.

Un raisonnement (de caractère général) montre que l'existence de l'inverse de ρ entraîne *la possibilité et la détermination* [1]), *de la* **division** *par* ρ (inverse de la multiplication) et, notamment la détermination de cet inverse lui-même (*quotient* de la division par ρ de l'élément unité):

$$\xi\times\rho = \sigma \quad \Leftrightarrow \quad (\xi\times\rho)\times\rho^{-1} = \sigma\times\rho^{-1} \quad \Leftrightarrow \quad \xi = \sigma\times\rho^{-1}.$$

L'ensemble des *éléments non nuls*, de $\mathbf{R}(\theta)$, entre lesquels existe une *multiplication* associative, et commutative, ainsi que l'opération inverse de *division*, est un **groupe** *multiplicatif abélien.*

[1]) Par *possibilité* on entend qu'il existe un quotient; par *détermination*, on entend que ce quotient est unique.

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:

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

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

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

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 **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'.

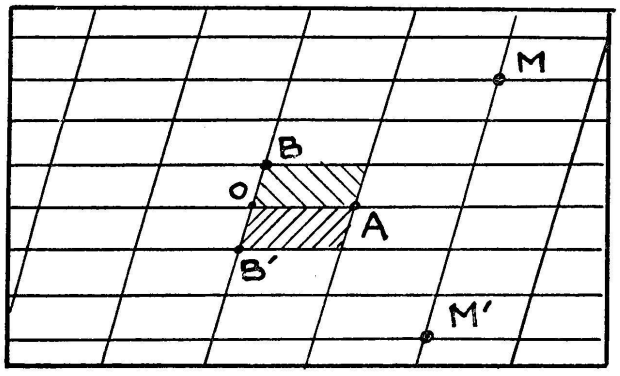
Un entier $\xi = x+y\theta$, de coordonnées x,y, nombres entiers, est égal à la somme de $|x|$ éléments égaux à $+1$, ou à -1 (suivant le signe de x), et de $|y|$ éléments égaux à θ, ou à $-\theta$ (suivant le signe de y). Le conjugué ξ' est obtenu de la même façon en remplaçant θ par θ'. En outre les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

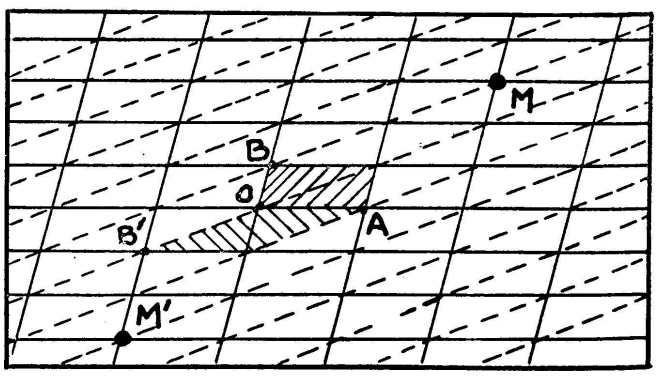
il y a une *correspondance biunivoque* entre les entiers ξ, du corps et les couples x,y de nombres entiers (qui en sont les coordonnées);

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

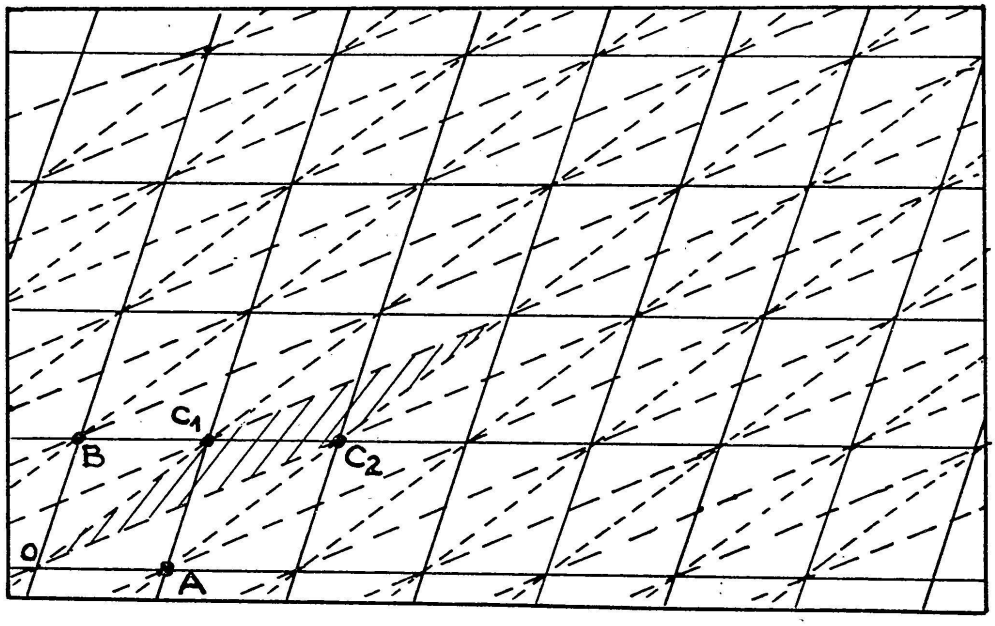
$$\overrightarrow{OM} = x.\overrightarrow{OA}+y.\overrightarrow{OB};\quad \overrightarrow{OM'} = x.\overrightarrow{OA}+y.\overrightarrow{OB'};$$
$$(\overrightarrow{OB'} = S.\overrightarrow{OA}-\overrightarrow{OB}).$$

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).

5. Congruence fondamentale (module premier).

L'arithmétique d'un corps quadratique $\mathbf{R}(\theta)$ est intimement liée à l'étude de son polynôme fondamental, considéré dans l'*anneau des nombres entiers, définis à un module entier m près*, —ou des *classes d'entiers*, mod. *m*—. C'est cette étude que précisent les définitions et les propriétés suivantes.

DÉFINITIONS. — On appellera **congruence fondamentale**, mod. m, de $\mathbf{R}(\theta)$, l'équation congruentielle, obtenue en écrivant que le polynôme fondamental du corps $F(x)$, est *congru* à 0, mod. m:

$$x^2 - Sx + N \equiv 0, \quad (\text{mod. } m).$$

L'étude de cette équation en x, consiste à chercher les valeurs entières c, de la variable x, telles que $F(c)$, qui est un nombre entier, soit divisible par m. S'il en existe, elles se répartissent en progressions arithmétiques, de raison m, doublement illimitées:

$$c + \lambda m; \qquad \lambda \text{ nombre entier quelconque.}$$

En effet l'égalité:

$$F(c+\lambda m) = F(c) + m \times (\text{un nombre entier}),$$

montre que tous les nombres entiers $F(c+\lambda m)$ sont divisibles par m, s'il en est ainsi de l'un d'eux.

Une telle progression, $c+\lambda m$, est couramment appelée une *classe d'entiers, mod. m* —ou un *entier défini, mod. m*— .

On appellera **zéro, mod.** m, de $F(x)$ —ou *solution* de la congruence fondamentale— indifféremment: *une progression* $c+\lambda m$, dont chaque terme donne à $F(x)$ une valeur $F(c+\lambda m)$ divisible par m; ou *un seul des termes* de cette progression, choisi arbitrairement, ou précisé par une condition convenable.

On peut d'abord établir une propriété générale, valable pour tout module m.

THÉORÈME des zéros conjugués. — Les solutions de la congruence fondamentale, s'il en existe, forment *un, ou plusieurs*,

couples de zéros mod. m, de $F(x)$. *Les deux zéros d'un couple ont une somme congrue à* S, mod. m:

$$c = c_0+\lambda m, \quad c' = c'_0+\lambda' m; \qquad c+c' \equiv S, \quad (\text{mod. } m);$$

ils sont appelés **conjugués** et désignés par une même lettre avec et sans accent (comme les éléments conjugués du corps).

Deux zéros conjugués sont égaux si et seulement si m est diviseur du discriminant D; leur valeur commune est alors appelée **zéro double.**

L'existence d'un zéro c entraîne celle de son conjugué c', car, d'après les calculs évidents de congruences, mod. m:

$$\left.\begin{array}{l} c+c' \equiv S, \\ \text{et} \\ c^2-Sc+N \equiv 0 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} c\times c' \equiv c\times(S-c) \equiv \mathrm{N} \\ \qquad\qquad\qquad\qquad (\text{mod. } m) \\ F(x) \equiv (x-c)\times(x-c') \end{array}\right.$$

En outre la congruence:

$$(c-c')^2 \equiv S^2-4N = D, \quad (\text{mod. } m),$$

montre que les deux zéros sont congrus —ou les deux progressions sont égales—, si et seulement si D est congru à 0, mod. m.

Pour qu'un zéro soit double il faut et il suffit qu'il annule, mod. m, le polynôme dérivé:

car:
$$\dot{F}(x) = 2x-S;$$
$$c \equiv c' \Leftrightarrow 2c \equiv S, \quad (\text{mod. } m).$$

On peut remarquer que ces calculs de congruences peuvent, aussi bien, être considérés comme des calculs [d'addition, soustraction et multiplication] entre les m classes d'entiers, mod. m:

$$0+\lambda m,\ 1+\lambda m,\ \ldots,\ (m-1)+\lambda m,$$

qui constituent un *anneau commutatif avec unité* —ou au sens restreint— .

Théorème de la congruence fondamentale pour un module premier. — Lorsque le module de la congruence fondamentale est un nombre premier p,

1. Si p *ne divise pas* le discriminant D:
ou bien la congruence est *impossible*;

ou bien elle a un et un seul couple de solutions inégales —ou $F(x)$ a *un et un seul couple de zéros conjugués incongrus*— ;

2. Si p *est diviseur* de D (notamment si $p = 1$), la congruence a deux solutions confondues —ou $F(x)$ a *un et un seul zéro double*— .

La première partie du théorème peut être complétée par des *propriétés caractéristiques de possibilité*:

pour un module premier p *impair*, ne divisant pas le discriminant D, la congruence fondamentale est possible, si, et seulement si, *il existe un entier, dont le carré soit congru à* D, *mod.* p. On exprime parfois cette existence en disant que D est **résidu quadratique** du nombre premier p.

pour le *module premier* 2, si le discriminant est impair, le polynôme fondamental est de la forme:

$$F(x) = x^2+x+N; \quad [S = -1; \quad D = 1-4N];$$

la congruence fondamentale est possible si, et seulement si, N *est pair*. Les deux zéros conjugués de $F(x)$ sont 0 et 1, (mod. 2).

1. Lorsque m est égal à un nombre premier p, pair ou impair, si la congruence est possible, le polynôme $F(x)$ a, au moins, un couple de zéros (conjugués), c et c', peut être égaux, et il est congru à un produit de binômes. *Il n'a pas alors d'autre zéro*, car la congruence

$$(x-c)\times(x-c') \equiv 0, \quad (\text{mod. } p),$$

exige que l'un au moins des facteurs soit divisible par p, c'est-à-dire que x soit congru à c ou à c'.

On peut exprimer ce raisonnement en disant que l'*anneau des* p *classes d'entiers, mod.* p, est un **domaine d'intégrité**, c'est-à-dire qu'un produit de deux facteurs ne peut être nul, que s'il en est ainsi de (au moins) l'un des facteurs. [C'est même un **corps**, car tout élément non nul, y possède un inverse.]

Pour un module p, *premier impair*, on peut utiliser le produit du polynôme $F(x)$ par 4:

$$4F(x) = (2x-S)^2-D;$$

l'existence d'un zéro est équivalente à celle d'un nombre entier $(2c—S)$, dont le carré est congru à D, mod. p.

Pour le *module premier* $p = 2$, il n'y a que deux classes d'entiers, représentés respectivement par 0 et 1; il suffit de former les valeurs qu'elles donnent à $F(x) = x^2+x+N$:

$$F(0) \equiv F(1) \equiv N, \quad (\text{mod. } 2);$$

d'où la condition d'existence.

2. Pour un *module premier impair* p, *diviseur de* D, l'expression de $4F(x)$ est congrue à:

$$4F(x) = (2x—S)^2—D \equiv (2x—S)^2, \quad (\text{mod. } p);$$

elle montre qu'il existe un et un seul zéro c, mod. p, qui rend $(2c—S)$ divisible par p. Suivant le cas, il est congru à:

$$c \equiv 0, \quad \text{si } S = 0; \qquad c \equiv \frac{p—1}{2}, \quad \text{si } S = —1.$$

Pour le *module* 2, lorsque D est pair, S est nul, la congruence:

$$x^2+N \equiv 0, \quad (\text{mod. } 2)$$

a une et une seule solution (zéro double), congrue à:

$$0, \quad \text{si } N \text{ est pair}; \qquad 1, \quad \text{si } N \text{ est impair}.$$

Pour $p = 1$, la propriété est triviale, il n'y a qu'une seule classe, formée de tous les nombres entiers et elle est zéro double de $F(x)$.

6. Congruence fondamentale (module composé).

On considère d'abord un *module primaire* —ou puissance d'un nombre premier > 1— .

Théorème de la congruence fondamentale pour un module primaire. Relativement à un *module* p^h, puissance (d'exposant h, entier positif), d'un nombre premier p, différent de 1, le polynôme fondamental $F(x)$:

1° *n'a pas de zéro*, pour tout exposant h, s'il n'en a pas pour $h = 1$ —ou si la congruence est impossible, mod. p— ;

2° *n'a pas de zéro*, pour h supérieur à 1, s'il a un *zéro double* pour $h = 1$ —ou si D est divisible par p— ;

3° a un et un seul *couple de zéros conjugués, incongrus*, s'il en est ainsi pour $h = 1$ —ou si la congruence est possible, mod. p; et p non diviseur de D— .

Les trois conditions suffisantes énumérant tous les cas possibles, le théorème exprime une *propriété caractéristique d'existence des zéros.*

1. S'il existe un zéro c_h, mod. p^h, il l'est, à fortiori, mod. p; c'est la propriété contraposée de l'énoncé.

2. Dans le cas d'un *module premier impair* p, différent de 1, diviseur du discriminant D, on peut encore utiliser $4F(x)$. Tout zéro, c, mod. p^h, l'est, à fortiori, mod. p; il rend $(2x—c)$ divisible par p et $(2x—S)^2$ divisible par p^2, d'où la congruence:

$$4F(c) = (2c—S)^2—D \equiv —D, \quad (\text{mod. } p^2).$$

L'existence d'un zéro c, mod. p^h, pour $h > 1$; donc, à fortiori, mod. p^2; entraînerait la divisibilité de D par p^2, ce qui est contraire à la définition du polynôme fondamental, dont le discriminant ne peut avoir de facteur carré impair.

Dans le cas du *module* 2^h et d'un polynôme de *discriminant pair*, donc de la forme x^2+N, tout zéro, mod. 2^h, donc, à fortiori mod. 2, ne peut être que de la forme:

$$0+2\lambda, \quad \text{si } N \text{ est pair}; \qquad 1+2\lambda, \quad \text{si } N \text{ est impair.}$$

Les valeurs de $F(x)$, pour ces nombres, sont congrues à

$$(2\lambda)^2+N \equiv N, \qquad (1+2\lambda)^2+N \equiv 1+N, \quad (\text{mod. } 4).$$

L'existence d'un zéro; mod. 2^h, pour $h > 1$; donc, à fortiori, mod. 4; entraînerait la divisibilité de N, ou de $1+N$, par 4; ce qui est aussi contraire à la définition du polynôme fondamental (**1**), puisque, dans le premier cas $N = —d$, est sans diviseur carré, et que dans le second cas $1+N = 1—d$ n'est pas divisible par 4.

3. On peut établir la propriété par récurrence sur h, en supposant qu'il existe un et un seul couple de zéros, c_h c'_h, conjugués, incongrus, mod. p^h (ce qui est vrai pour $h = 1$). S'il en existe mod. p^{h+1}, ils le sont, à fortiori, mod. p^h, donc de l'une des formes:

$$c_h+\lambda p^h, \qquad \text{ou} \qquad c'_h+\lambda' p^h; \qquad \lambda,\lambda' \text{ entiers.}$$

On calcule les valeurs qu'ils donnent à $F(x)$; pour le premier:

$$F(c_h+\lambda p^h) \equiv F(c_h)+\lambda p^h.\dot{F}(c_h), \quad (\text{mod. } p^{h+1});$$

on a supprimé des termes du développement en λ, qui sont multiples de p^{2h}, donc à fortiori, de p^{h+1}. La valeur ainsi obtenue est divisible par p^h, il suffit de chercher si son quotient par cette puissance peut être divisible par p, d'où la congruence:

$$|F(c_h): p^h|+\lambda.\dot{F}(c_h) \equiv 0, \quad (\text{mod. } p).$$

Or c_h étant zéro, mod. p_h, l'est aussi mod. p et il ne peut être double, en raison de la propriété 2, précédente. La dérivée, coefficient de λ, n'est donc pas nulle, mod. p, cette équation du premier degré en λ a une et une seule solution, qui peut être désignée par λ_h, on obtient ainsi un zéro déterminé:

$$c_{h+1} \equiv c_h+\lambda_h p^h, \quad (\text{mod. } p^{h+1}).$$

On obtient de même un zéro déterminé $c'_h+\lambda'_h.p^h$, de la deuxième forme; ces deux zéros sont incongrus, puisque leur différence:

$$c_{h+1}-c'_{h+1} \equiv c_h-c'_h, \quad (\text{mod. } p^h)$$

n'étant pas divisible par p^h, ne peut l'être par p^{h+1}. Comme ce sont les deux seuls zéros, ils sont conjugués et leur somme est congrue à S.

L'application de la récurrence, depuis $h = 1$, permet d'écrire ces zéros, en partant des zéros, mod. p:

$$\left.\begin{aligned} c_{h+1} &\equiv c_1+\lambda_1 p+\ldots+\lambda_h p^h, \\ c'_{h+1} &\equiv c'_1+\lambda'_1 p+\ldots+\lambda'_h p^h; \end{aligned}\right\} \quad (\text{mod. } p^{h+1}).$$

La somme de ces deux développements, limités à l'indice k, est congrue à S, mod. p^{k+1} [1].

THÉORÈME de la congruence fondamentale pour un module composé. — Pour un module égal au produit de plusieurs puissances de nombres premiers différents:

$$m = \Pi m_i; \quad m_i = p_i^{hi}; \quad p^i \text{ premier} \neq 1; \quad i \text{ de } 1 \text{ à } s;$$

le polynôme fondamental a des couples de zéros conjugués si et seulement si:

1° pour tout facteur premier p_i, *diviseur du discriminant* D, *l'exposant* h_i *est égal à* 1 ($m_i = p_i$);

2° pour tout facteur premier p_j, *premier avec* D, *la congruence, mod.* p_j, *est possible* —ou le polynôme a deux zéros conjugués incongrus— .

Si ces deux conditions sont remplies et si $s' \leqslant s$ est le nombre de facteurs premiers p_j (ou m_j) premiers avec D, il y a $2^{s'}$ *zéros incongrus*. Si s' n'est pas nul, ils sont répartis en $2^{s'-1}$ *couples de zéros conjugués*; si $s' = 0$; ils se réduisent à un *zéro double*; m étant d'ailleurs alors diviseur de D.

Les conditions sont *nécessaires*: si l'une, au moins, n'était pas vérifiée pour un facteur m_i, ou m_j, le polynôme n'aurait pas de zéro relativement à ce facteur, donc, à fortiori, relativement au module m, qui en est un multiple.

Les conditions sont *suffisantes*: pour chaque facteur m_i, diviseur de D, le polynôme $F(x)$ a un zéro c_i (double); pour chaque facteur m_j, premier avec D, il a deux zéros (conjugués) c_j et c_j'. Tout zéro c de $F(x)$, mod. m, doit alors vérifier l'un des systèmes de s congruences:

$$c \equiv c_i, \quad (\text{mod. } m_i); \qquad c \equiv c_j \quad \text{ou} \quad c \equiv c_j', \quad (\text{mod. } m_j).$$

---

[1]) La démonstration de cette existence aurait pu être faite sans utiliser nommément la dérivée $\dot{F}(x)$. Sous la forme adoptée, elle est valable pour un polynôme $F(x)$, de degré quelconque, à coefficients entiers et normé. Si ce polynôme a, relativement à un module premier p, un zéro c, qui n'annule pas sa dérivée $\dot{F}(x)$, il a, relativement à tout module p^h (h entier positif), un zéro c^h congru à c, mod. p. Cette propriété, qui peut encore être énoncée sous une forme plus générale (existence d'un polynôme, de degré quelconque diviseur de $F(x)$), est connue sous le nom de *lemme de* HENSEL.

Chacun des systèmes a une solution déterminée, mod. m, puisque les s modules m_i sont premiers entre eux deux à deux et que leur produit est égal à m [1].

Dans la formation d'un système de congruences, pour chacun des s' modules m_j, premiers avec D, on peut choisir entre deux congruences. Il y a donc bien $2^{s'}$ systèmes, d'où le nombre de zéros indiqué. Leur répartition en couples conjugués en résulte; on passe d'ailleurs d'un zéro c à son conjugué c', en changeant le choix dans chacune des congruences, mod. m_j.

Pour m diviseur de D et sans facteur carré, il n'y a qu'un système de s congruences, qui détermine un zéro double. Il peut être obtenu par les règles suivantes:

$$\begin{array}{ll} D \text{ impair; } m \text{ impair} & \\ D = 4d;\ d \text{ impair, } m \text{ pair:} & c \equiv (m+S):2 \begin{cases} \equiv (m-1):2, & (\text{mod. } m); \\ \equiv m:2, & (\text{mod. } m); \end{cases} \\ D = 4d;\ m \text{ diviseur de } d; & c \equiv 0, \quad (\text{mod. } m). \end{array}$$

7. Idéaux canoniques.

L'extension de la théorie de la *divisibilité* (arithmétique) à un corps quadratique $\mathbf{R}(\theta)$ et au domaine de ses entiers (algébriques) $\mathbf{E}(\theta)$ a conduit à considérer, dans $\mathbf{R}(\theta)$, des sous-ensembles particuliers, appelés *idéaux*.

On peut donner d'un idéal une *définition constructive*, en le caractérisant par deux de ses éléments, convenablement choisis, qui en constituent une *base canonique* et, à partir desquels, il est

---

[1]) La résolution d'un système de deux congruences:

$$x \equiv a_1, \quad (\text{mod. } m_1) \qquad x \equiv a_2, \quad (\text{mod. } m_2);$$

est équivalent à la résolution de l'équation en λ:

$$a_1 + \lambda m_1 \equiv a_2, \quad (\text{mod. } m_2);$$

elle est possible et déterminée si m_1 et m_2 sont premiers entre eux et la solution du système est de la forme:

$$a_1 + (\lambda_1 + u m_2) \times m_1 = b + u \times (m_1 \times m_2);$$

elle est déterminée, [module $m = m_1 \times m_2$].

Cette construction s'étend, de proche en proche, ou par récurrence sur s, à un système de s congruences dont les modules sont premiers entre eux deux à deux.

engendré par additions et soustractions. On peut alors établir des propriétés —ou qualités— caractéristiques d'*appartenance* d'un tel ensemble.

On peut, inversement, utiliser ces qualités caractéristiques, pour donner d'un idéal une *définition axiomatique*, dont il est possible de déduire sa définition constructive, c'est-à-dire sa génération par une base canonique [1];

On peut encore établir sa génération par d'*autres bases*, qualifiées *arithmétiques libres*, équivalentes arithmétiquement à la base canonique; ou encore par des *bases*, non présumées libres, d'un nombre plus grand de termes.

On va étudier d'abord une famille d'idéaux particuliers, appelés *canoniques*; ils permettent de construire et de caractériser les idéaux les plus généraux, appelés *fractionnaires* (comprenant les idéaux *entiers*.

7. 1. DÉFINITION constructive. — Dans un corps quadratique $\mathbf{R}(\theta)$, caractérisé par un polynôme fondamental dont un des zéros θ, est pris pour *générateur*, un **idéal canonique M** peut être défini par:

---

[1]) Dans certaines conceptions de la *divisibilité arithmétique* usuelle, c'est-à-dire dans le corps **R** des nombres rationnels et du domaine **E** de ses nombres entiers, on considère d'abord un sous-ensemble $r \times \mathbf{E}$ (parfois noté (r)), des *multiples* d'un nombre (rationnel) r, c'est-à-dire des produits $r \times x$, du nombre r par tous les nombres entiers x. Il est manifeste qu'un tel ensemble contient les *différences mutuelles* de ses termes et *leurs produits par tout entier*.

Mais inversement si un ensemble de nombres rationnels, dont *les valeurs absolues sont limitées inférieurement*, vérifie ces propriétés d'appartenance, c'est-à-dire contient tout les éléments $x_1 \times r_1 + x_2 \times r_2$ (x_1, x_2 entiers arbitraires) construits par additions et soustractions au moyen de tout couple r_1, r_2 de ses éléments, il est égal à l'ensemble $r \times x$, des multiples d'un de ses éléments r convenablement choisi; le plus petit en valeur absolue, qui peut être pris positif.

Cette propriété dont la démonstration résulte de la construction de la *division euclidienne* —ou de la *partie entière* d'une fraction— est une des formes de la *propriété fondamentale de la divisibilité* (des nombres rationnels); elle entraîne notamment l'existence du *p.g.c.d.* (et du *p.p.c.m.*) de plusieurs nombres rationnels. On en trouvera ci-dessous une démonstration explicite, dans une circonstance qui n'est particulière qu'en apparence: construction de la norme d'un idéal canonique, défini axiomatiquement.

un nombre entier positif m, appelé la **norme** de **M**; *tel que la congruence fondamentale soit possible*, mod. m;

une progression arithmétique $c+\lambda m$, de raison m, —ou un entier, défini, mod. m— , *dont les termes*, qui seront appelés les **racines** de **M**; *constituent un zéro*, de cette congruence (**5**):

$$F(c) \equiv 0, \quad (\text{mod. } m) \quad \Leftrightarrow \quad F(c+\lambda m) \equiv 0, \quad (\text{mod. } m).$$

Une racine c étant choisie arbitrairement, l'idéal canonique **M** *est l'ensemble des éléments de* **R**(θ), construits par additions et soustractions, au moyen du couple m, θ—c; c'est-à-dire des valeurs de la forme de m et θ—c, dont les valeurs des variables sont des nombres entiers.

$$\xi = x\times m+y\times(\theta—c) = \|x\ y\|\times\left\|\begin{matrix} m \\ \\ \theta—c \end{matrix}\right\|; \qquad x, y \text{ nombres entiers.}$$

Les éléments ξ, ainsi construits sont des *entiers* (*particuliers*) *du corps*; l'idéal est *un sous-ensemble de* **E**(θ).

Un tel couple de termes sera appelé une **base canonique** *de l'idéal*, qui sera désigné lui-même par ce couple entre parenthèses

$$\mathbf{M} = (m, \theta—c); \qquad [F(c) \equiv 0, \quad (\text{mod. } m)].$$

Les nombres entiers x,y, qui sont déterminés, pour un élément ξ, sont encore appelés ses **coordonnées**, *relativement à cette base.*

On emploie ainsi un vocabulaire et une construction, analogues à ceux qui ont été employés pour le domaine **E**(θ) des entiers du corps: l'élément ξ, de **M**, de coordonnées x,y, est égal à la somme de $|x|$ éléments égaux à m, ou à $—m$, et de $|y|$ éléments égaux à (θ—c), ou à ($—\theta+c$).

La *détermination* des coordonnées x,y résulte de l'équivalence:

$$x\times m+y\times(\theta—c) = x'\times m+y'\times(\theta—c)$$
$$\Leftrightarrow \quad [(x—x')\times m — (y—y')\times c]+(y—y')\times\theta = 0;$$

en raison des règles de calcul dans **E**(θ), la deuxième forme de l'égalité entraîne la nullité de $y—y'$, donc aussi de $x—x'$; donc:

$$y = y' \quad \text{et} \quad x = x'.$$

Il y a *correspondance biunivoque* entre les éléments de l'idéal et les couples de nombres entiers x,y (qui en sont les coordonnées).

Dans un corps $\mathbf{R}(\theta)$, de générateur θ, le sous-ensemble **M** est indépendant de la base canonique adoptée pour le construire, c'est-à-dire du choix de la racine c, dans sa progression; quand on la remplace par $c_1 = c+hm$, les coordonnées des éléments restent des nombres entiers:

$$x\times m+y\times(\theta-c) = (x+yh)\times m+y\times(\theta-c_1).$$

Dans un idéal canonique **M**, ainsi construit et considéré comme un ensemble d'entiers du corps $\mathbf{R}(\theta)$, on peut caractériser la construction de la *norme* et des *racines*:

la norme, d'un idéal canonique **M**, *est égale au minimum* (effectivement atteint) *des valeurs absolues des entiers rationnels*, non nuls, qui lui appartiennent —ou au plus petit de ceux qui sont positifs— ;

les racines sont égales aux entiers rationnels c, de $\mathbf{R}(\theta)$, pour lesquels les différences $\theta-c$ appartiennent à **M**.

D'une part, un élément de **M**:

$$x\times m+y\times(\theta-c) = (x\times m-y\times c)+y\times\theta,$$

est un entier rationnel si, et seulement si, y est nul et il est égal à $x\times m$. La plus petite des valeurs absolues de ces entiers $|x\times m| = |x|\times m$ est m, qui est aussi égal au plus petit entier positif $1\times m = m$.

D'autre part les entiers rationnels u, pour lesquels $\theta-u$ appartient à **M**, vérifient la condition:

$$\theta-u = x\times m+y\times(\theta-c) \Leftrightarrow [x\times m-y\times c+u]+(y-1)\times\theta = 0;$$

dans laquelle x,y sont des nombres entiers. Il en résulte:

$$y = 1 \quad \text{et} \quad u = c-x\times m \quad \text{(termes de la progression)}.$$

Le domaine $\mathbf{E}(\theta)$ de tous les entiers rationnels du corps (**3**) *est un idéal canonique, trivial*, construit avec la base $1\ \theta-0$, ou $1\ \theta$; sa norme est égale à 1, la progression de ses racines est celle des nombres entiers, qui est bien zéro de $F(x)$, mod. 1.

7. 2. *Définition axiomatique d'un idéal canonique.*

Comme il a été dit, on peut caractériser un idéal canonique par certaines conditions d'appartenance, qui sont caractéristiques.

Théorème caractéristique d'un idéal canonique. — *Pour qu'un ensemble* **M**, d'entiers du corps **R**(θ), *soit un idéal canonique, il faut et il suffit que*:

1. *Il contienne les différences*, donc aussi les sommes, *mutuelles de ses éléments*;

2. *Il contienne des éléments de la forme* θ—c, c'est-à-dire des entiers du corps, dont le coefficient de θ soit égal à 1 (il suffit qu'il en contienne au moins un);

3. *Il contienne tout produit de chacun de ses éléments par tout entier du corps* (et notamment les produits mutuels de ses éléments).

En langage de l'algèbre moderne, ces conditions peuvent être énoncées;

1. **M** *est un module* —ou un groupe additif— ;
2. L'ensemble **M**—θ contient des entiers rationnels;
3. **M** × entier du corps ⊂ **M**.

Les conditions sont *nécessaires*: les deux premières sont manifestement remplies par un ensemble **M** d'éléments engendrés par une base canonique.

Pour vérifier la troisième, on peut calculer $(\theta—c)^2$, en utilisant notamment la formule de Taylor, appliquée à $F(x)$, dans le corps **R**(θ):

$$0 = F(\theta) = (\theta—c)^2+(2c—S)\times(\theta—c)+F(c).$$

Comme $F(c)$ est un multiple de m, il en résulte une construction de $(\theta—c)^2$ au moyen de la base canonique:

$$(\theta—c)^2 = a\times m+b\times(\theta—c);$$
$$[a = —F(c):m, \quad —b = 2c—S, \quad \text{nombres entiers}]$$

On peut alors calculer le produit d'un élément de **M**, par un entier de **R**(θ), dont on peut prendre pour base 1 et θ—c:

$$[x\times m+y\times(\theta—c)]\times[x'+y'\times(\theta—c)]$$
$$= (xx'+yy'a)\times m+(xy'm+yx'+yy'b)\times(\theta—c);$$

c'est bien un élément de **M**, engendré par la base m, $\theta—c$, avec les coefficients entiers:

$$xx'+yy'a, \quad xy'm+yx'+yy'b.$$

Les conditions sont *suffisantes*: dans un ensemble $\mathbf{M}_1$, qui les vérifie, on va d'abord construire la *norme*, en appliquant la propriété de détermination qui en a été donnée.

$\mathbf{M}_1$ contient des entiers rationnels non nuls, notamment:

$$(\theta—c)\times(\theta'—c) = F(c),$$

qui est le produit d'un élément $\theta—c$, dont l'existence dans $\mathbf{M}_1$ résulte de la condition 2, par son conjugué $\theta'—c$, qui est un entier du corps. Pour ces entiers, il existe un minimum m, effectivement atteint, de leurs valeurs absolues. On va vérifier qu'ils sont égaux aux multiples $x\times m$, de ce minimum.

D'une part, en raison de la condition 1, les entiers rationnels $+m$, $—m$ et tous ceux $x\times m$ qui en sont déduits par additions et soustractions appartiennent à $\mathbf{M}_1$.

D'autre part pour toute valeur z, d'un entier rationnel de $\mathbf{M}_1$, on peut effectuer sa division (euclidienne) par l'entier m:

$$r = z—x\times m; \quad 0 \leqslant r < m; \quad x \text{ nombre entier.}$$

Comme les valeurs z et $x\times m$ sont égales à des entiers rationnels de $\mathbf{M}_1$ il en est de même de leur différence r, qui est nulle puisqu'elle est inférieure au minimum m, des valeurs absolues non nulles; donc $z = x\times m$.

Ce premier point étant acquis, reste à vérifier que $\mathbf{M}_1$ est bien engendré au moyen des éléments: $\theta—c$ déjà utilisé et m, qui vient d'être construit. D'une part toute valeur ainsi obtenue:

$$x\times m+y\times(\theta—c); \quad x,y \text{ nombres entiers}$$

appartient à $\mathbf{M}_1$, en raison de la condition 1.

D'autre part tout élément de $\mathbf{M}_1$ étant un entier du corps peut être mis sous la forme:

$$\xi = x'+y'\theta = (x'+y'c)+y'\times(\theta—c); \quad x'+y'c = \xi—y'\times(\theta—c).$$

Le nombre entier $x'+y'c$, qui est égal à la différence de deux éléments de $\mathbf{M}_1$ appartient aussi à $\mathbf{M}_1$ et en est un entier rationnel; il est donc bien égal à un multiple $x_1\times m$, de m.

On vérifie encore que c, donc tout terme de la progression $c+\lambda m$, est *zéro de la congruence fondamentale*: c'est une conséquence de la première remarque utilisée: la valeur $F(c)$ étant égale à un entier rationnel de $\mathbf{M}_1$, est multiple de m.

7. 3. *Idéaux conjugués.*

Comme pour la construction d'un corps quadratique et de son domaine d'entiers (**1** et **3**), un idéal canonique peut être engendré en utilisant indifféremment les générateurs θ et θ', (zéros du polynôme fondamental) mais sous la réserve de leur associer respectivement les zéros conjugués de la congruence fondamentale, dont le module est la norme de l'idéal. On peut exprimer ceci par la formation des bases canoniques:

Un idéal canonique a *deux suites de bases canoniques*, définies par *la même norme m et les différences* θ—c et θ'—c', des générateurs du corps et des zéros conjugués c, c', (progressions de raison m), de la congruence fondamentale:

$$(m,\ \theta—c) = (m,\ \theta'—c');$$

Les constructions des termes de ces différences (zéros du polynôme et zéros de la congruence) peuvent être exprimées par les formules:

$$\begin{array}{llll} \theta+\theta' = S; & \theta\times\theta' = N; & \text{dans le corps;} \\ c+c' \equiv S; & c\times c' \equiv N; & (\text{mod. } m). \end{array}$$

L'égalité des éléments construits avec ces deux bases est assurée par une correspondance biunivoque de leurs coordonnées, relativement à chacune d'elles:

$$x\times m+y\times(\theta—c) = x'\times m—y\times(\theta'—c');.$$
$$x'—x = y\times[(c+c'—S):m].$$

Cette propriété conduit à la conception de la conjugaison des idéaux canoniques et à sa définition, constructive et axiomatique.

Définition (constructive). — *Deux idéaux canoniques sont appelés* **conjugués**, et seront désignés par la même lettre, avec et sans accent, *lorsqu'ils sont engendrés*: par une même norme,

avec les mêmes racines, mais avec les générateurs conjugués θ et θ', du corps:

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

c'est-à-dire encore *par des bases canoniques conjuguées* [**2**].

Il est équivalent de dire (définition axiomatique) que *deux idéaux canoniques conjugués sont constitués par des éléments* (entiers du corps) *respectivement conjugués* [**3**]; définis par des coordonnées égales, relativement aux bases conjuguées; car:

$$\xi = \|x\ y\| \times \begin{Vmatrix} m \\ \theta - c \end{Vmatrix} \in \mathbf{M} \quad \Leftrightarrow \quad \xi' = \|x\ y\| \times \begin{Vmatrix} m \\ \theta' - c \end{Vmatrix} \in \mathbf{M}'.$$

En appliquant une remarque précédente, il est encore équivalent de *caractériser deux idéaux conjugués*, relativement à un même générateur θ du corps, *par deux zéros conjugués*, c et c', *de la congruence fondamentale* [**5**]:

$$\mathbf{M} = (m,\ \theta - c); \quad \mathbf{M}' = (m,\ \theta - c'); \quad c + c' \equiv S, \pmod{m}.$$

Il suffit, en effet, dans la base précédente de $\mathbf{M}'$, de remplacer $\theta' - c$ par la différence du générateur conjugué de θ' et d'un zéro conjugué de c.

Un idéal canonique est **double**, lorsqu'il est égal à l'idéal conjugué, c'est-à-dire lorsque *ses racines sont un zéro double de la congruence*; ce qui a lieu si, et seulement si, sa norme m est diviseur du discriminant D (**5.** théorème des zéros conjugués).

L'idéal canonique trivial $\mathbf{E}(\theta)$ est double.

7. 4. *Racines minimum.*

Comme il a déjà été dit (**5**); dans la progression $c + \lambda m$ des racines d'un idéal, de norme m, on peut *distinguer* —ou choisir— une racine particulière, notamment en précisant qu'elle appartient à un segment déterminé, de longueur m, dont une extrémité est exceptée, s'il y a lieu. Il y a intérêt, ainsi qu'il sera dit plus loin (**21**), à ce que ce choix soit fait simultanément pour l'idéal et son conjugué; ils ont même norme m et la somme de leurs

racines est congrue à S, mod. m. Pour cette raison on choisira un segment, de longueur m et de milieu $S:2$ (0 ou $-1:2$). On vérifie aisément qu'une racine ainsi déterminée est aussi de valeur absolue minimum dans sa progression. C'est cette condition qu'exprime la définition suivante.

DÉFINITION. — *On appelle* **racine minimum**, d'un idéal canonique, de norme m, et on note avec une *surligne*, *celle de ses racines qui vérifie la condition de comparaison*:

$$\frac{S-m}{2} < \bar{c} \leqslant \frac{S+m}{2} \qquad \text{ou} \qquad -m < 2\bar{c} - S \leqslant m.$$

Cette condition est encore équivalente à l'alternative:

$$|2\bar{c}-S| < m, \qquad \text{ou bien:} \quad 2\bar{c}-S = m.$$

On peut préciser cette limitation, suivant les divers cas, pour les racines minimum de deux idéaux conjugués et vérifier qu'elles sont bien déterminées.

Pour un idéal double —ou deux idéaux conjugués égaux— toute racine c rend $2c-S$ divisible par la norme m. En se reportant à la construction des racines doubles (**6**), la *racine minimum* $\bar{c}$ est:

$$0\ [S = 0 \text{ et } m \text{ diviseur de } N] \qquad \text{ou} \qquad \frac{S+m}{2}$$

Si un idéal n'est pas égal à son conjugué, sa racine n'est pas double, $2c-S$ n'est pas divisible par m et, à fortiori, n'est pas nul. Pour deux idéaux conjugués inégaux, deux racines, de somme égale à S, donnent des valeurs opposées, donc une même valeur absolue à $2x-S$. Elles vérifient donc simultanément le premier terme de l'alternative de la condition de minimum. L'une d'elles est négative, elle sera notée de préférence par la lettre accentuée $\bar{c}'$, l'autre $\bar{c}$ est positive ou nulle. On en conclut la situation suivante de ces racines, relativement au segment adopté; ce qui met aussi en évidence leur détermination:

$$\bar{c}'-m < \bar{c}-m < \frac{S-m}{2} < \bar{c}' < 0 \leqslant \bar{c} < \frac{S+m}{2} < \bar{c}'+m < \bar{c}+m$$

8. Idéaux fractionnaires.

8. 1. *Définition constructive.*

Les *idéaux fractionnaires* —ou, plus simplement, les idéaux— d'un corps quadratique, peuvent être construits au moyen des idéaux canoniques, dont ils sont, par ailleurs, une généralisation.

DÉFINITION. — Dans un corps $\mathbf{R}(\theta)$, un **idéal fractionnaire I**, *non nul*, peut être défini par:

un nombre rationnel positif q, appelé son **facteur rationnel**;

un idéal canonique $\mathbf{M} = (m, \theta—c)$, appelé son **facteur canonique**.

L'idéal ainsi défini **I** est l'*ensemble des éléments* ρ, de $\mathbf{R}(\theta)$, obtenus en multipliant par le facteur rationnel q les éléments du facteur canonique **M**:

$$\rho = q \times \xi; \qquad \xi = x \times m + y \times (\theta — c); \qquad x,y \text{ nombres entiers.}$$

La génération des éléments peut être exprimée directement par les valeurs d'une forme, dont les valeurs des variables —ou les multiplicateurs— sont des nombres entiers:

$$\rho = \|x\ y\| \times \begin{Vmatrix} q \times m \\ q \times (\theta — c) \end{Vmatrix} \qquad \text{ou} \qquad \|x'\ y\| \times \begin{Vmatrix} q \times m \\ —q \times (\theta' — c') \end{Vmatrix}.$$

Les nombres entiers c et c' sont des termes de deux progressions arithmétiques, de raison m, de somme congrue à S. Les couples d'éléments générateurs $q \times m$, $q \times (\theta — c)$ sont encore appelés les **bases canoniques**, de l'idéal **I**, qui sera lui-même désigné par l'une des expressions, appelée sa **forme canonique**:

$$\mathbf{I} = q \times \mathbf{M}, \qquad \text{ou} \quad q \times (m, \theta — c), \qquad \text{ou} \quad q \times (m, \theta' — c').$$

Les nombres entiers x,y, qui sont déterminés pour chaque élément ξ de **M**, le sont aussi pour chaque élément $\rho = q \times \xi$, de **I**, car:

$$q \times \xi_1 = q \times \xi_2 \quad \Leftrightarrow \quad q \times (\xi_1 — \xi_2) = o \quad \Leftrightarrow \quad \xi_1 = \xi_2.$$

Ils seront encore appelés les *coordonnées* de l'élément ρ, relativement à la base canonique de **I**.

Un idéal canonique est, à fortiori, un idéal fractionnaire; il est égal à son facteur canonique; son facteur rationnel est $+1$ —ou il n'a pas de facteur rationnel « proprement dit » (différent de 1)— .

On appelle encore **idéal nul**, le sous-ensemble de $\mathbf{R}(\theta)$ constitué par *le seul élément nul*; il peut être considéré comme défini par un *facteur rationnel égal à* 0 et un *facteur canonique arbitraire.*

DÉFINITION. — La **norme** d'un idéal fractionnaire est (le nombre rationnel positif égal à) *le produit du carré du facteur rationnel par la norme du facteur canonique*:

$$\text{Norme de } [q \times (m,\ \theta\text{—}c)] = q^2 \times m.$$

Cette définition sera justifiée ci-dessous (**13**); elle comprend le cas d'un idéal canonique, pour lequel $q = 1$; elle s'étend à l'*idéal nul*, qui est le seul dont la norme soit nulle.

Dans un idéal fractionnaire **I**, non nul, ainsi construit et considéré comme un ensemble d'éléments $\rho = r+s\theta$, du corps $\mathbf{R}(\theta)$, on peut caractériser les termes de sa forme canonique, ainsi qu'il a été fait pour un idéal canonique (**7**).

Le *facteur rationnel*, d'un idéal **I**, *est égal au minimum*, effectivement atteint, *des valeurs absolues* $|s|$, des deuxièmes coordonnées —ou multiplicateurs de θ— des éléments [non rationnels] de **I**, (pour lesquels ces coordonnées s ne sont pas nulles). C'est aussi *le plus petit des facteurs rationnels* (**3**), des éléments non nuls de **I**.

Le facteur canonique est l'ensemble des quotients $\rho \times q^{-1}$, des éléments ρ, de **I**, par son facteur rationnel q. Ce sont des entiers du corps, qui constituent un idéal *canonique.*

Les expressions des éléments de **I** sont:

$$\rho = x \times (qm) + y \times [q \times (\theta\text{—}c)] = (x \times qm\text{—}y \times qc) + (y \times q)\theta.$$

Les multiplicateurs de θ sont $s = y \times q$, le minimum des valeurs absolues $|y \times q| = |y| \times q$, de ceux qui ne sont pas nuls, est manifestement q, et il est atteint pour tous les éléments où $y = 1$.

Le facteur rationnel de tout élément $\rho = q \times \xi$ est multiple de q (égal à son produit par le facteur rationnel de ξ), le plus petit est effectivement égal à q, puisqu'il est notamment celui de $q \times (\theta\text{—}c)$.

Les quotients $\rho \times q^{-1} = \xi$ sont les éléments du facteur canonique **M**.

8. 2. *Définition axiomatique d'un idéal fractionnaire.*

On peut encore caractériser un idéal fractionnaire par des conditions d'appartenance, ainsi qu'il a été fait pour un idéal canonique.

THÉORÈME caractéristique d'un idéal fractionnaire. — *Pour qu'un ensemble* **I**, d'éléments du corps $\mathbf{R}(\theta)$, *soit un idéal fractionnaire, il faut et il suffit que*:

1. *Il contienne les différences*, donc aussi les sommes, *mutuelles de ses éléments* —ou soit un *module*— ;

2. *Les facteurs rationnels*, de ses éléments non nuls (**3**), *soient limités inférieurement*;

3. *Il contienne tout produit de chacun de ses éléments par tout entier du corps* (mais non plus tout produit mutuel).

Les conditions 1 et 3 sont aussi celles qui ont été indiquées pour un idéal canonique (**7**); toutefois elles s'appliquent ici à des éléments qui ne sont plus nécessairement des entiers du corps.

La condition 2 pourrait être remplacée par la condition, plus restrictive, que les dénominateurs des facteurs rationnels, non nuls (mis sous forme irréductible), soient limités supérieurement et, par suite, en nombre fini. La condition 2 en résulterait évidemment; en outre on pourrait affirmer l'existence d'un nombre entier w (notamment le p.p.c.m. de ces dénominateurs) tel que tous les produits $w \times \rho$ soient des entiers du corps (en abrégé $w \times \mathbf{I} \subset \mathbf{E}(\theta)$).

Les conditions sont *nécessaires*: les appartenances 1 et 3, vérifiées par les éléments (entiers du corps) du facteur canonique **M**, le sont aussi, évidemment, par leurs produits par le facteur rationnel q.

D'autre part, les facteurs rationnels des éléments de **I** sont des *multiples* de q, les valeurs absolues de ceux qui ne sont pas nuls sont donc au moins égales à q.

Les conditions sont *suffisantes*: elles sont vérifiées par le *sous ensemble de* $\mathbf{R}(\theta)$, réduit au seul élément nul, qui, par définition est un idéal (trivial).

Si elles sont vérifiées par un ensemble **I**, qui contient des éléments non nuls, on peut d'abord construire le facteur q, en utilisant la détermination qui en a été donnée, en appliquant un raisonnement arithmétique, analogue à celui qui a été employé pour la norme d'un idéal canonique.

L'ensemble $\{s\}$ des coefficients s, de θ, dans les éléments ρ, de l'ensemble **I**, contient des éléments non nuls, car s'il existe dans **I** un élément rationnel r, non nul, il existe aussi l'élément $r\theta$, qui est son produit par l'entier (du corps) θ (condition 3). Cet ensemble contient les opposés de ses termes, $+s$ et $-s$, et leurs sommes —et différences— mutuelles; car la différence s_1-s_2 des coefficients de θ dans deux éléments ρ_1 et ρ_2, de **I**, est le coefficient de θ, dans la différence $\rho_1-\rho_2$, qui appartient aussi à **I**, d'après la condition 1.

On peut se borner à considérer les coefficients s positifs; ils sont limités inférieurement, puisqu'ils sont multiples des facteurs rationnels, eux-mêmes limités, d'après la condition 2. Ils ont une *limite inférieure* q; elle est effectivement atteinte, si non son voisinage contiendrait une infinité d'éléments de $\{s\}$ dont les différences mutuelles, appartenant aussi à $\{s\}$, seraient infiniment petites.

On peut alors constater que l'*ensemble* $\{s\}$ *est égal à l'ensemble des multiples* de q —ou des produits $x\times q$, par les nombres entiers x— .

D'une part ces multiples, construits par additions et soustractions au moyen de q, qui est élément de $\{s\}$ appartiennent à cet ensemble.

D'autre part tout élément s, de $\{s\}$, est de cette forme, car en lui retranchant le plus grand multiple de q, qui lui est au plus égal, on obtient la différence:

$$s' = s-q\times x; \qquad 0 \leqslant s' < q; \qquad x \text{ nombre entier};$$

elle appartient à $\{s\}$, ainsi que s et $x\times q$, et elle ne peut être que nulle puisqu'elle est inférieure à q et non négative.

On peut ensuite vérifier que, dans tout élément $\rho = r+s\theta$, de **I**, la coordonnée r, ou multiplicateur de 1, est aussi multiple de q. Il suffit de constater qu'il est égal au coefficient de θ, dans un autre élément de **I**, qui peut être construit en multipliant ρ par un entier du corps, ce qui est notamment le cas pour le produit:

$$(r+s\theta)\times(\theta-S) = -(Sr+Ns)+r\theta = r_1+r\theta; \qquad (r_1 \text{ rationnel}).$$

Tout élément ρ, de **I**, ayant ainsi des coordonnées multiples de q est, lui-même, égal au produit de q par un entier du corps:

$$\rho = r+s\theta = \rho \times \xi; \qquad \xi = x'+y'\theta; \qquad x',y' \text{ nombres entiers.}$$

L'ensemble **M**, de ces entiers ξ, est un *idéal canonique*, car il vérifie les conditions de la définition axiomatique:

1 et 3 puisque:

$$\rho_1,\rho_2 \in \mathbf{I} \Rightarrow \rho_1 - \rho_2 \in \mathbf{I} \Rightarrow [(\rho_1 \times q^{-1}) - (\rho_2 \times q^{-1})] \in \mathbf{M};$$
$$\alpha \in \mathbf{E}(\theta) \text{ et } \rho \in \mathbf{I} \Rightarrow \alpha \times \rho \in \mathbf{I} \Rightarrow [\alpha \times (\rho \times q^{-1})] \in \mathbf{M}.$$

2, puisque, d'après la construction de q, il existe dans **I**, un élément ρ_0, dont il est le coefficient de θ, de sorte que:

$$\rho_0 \times q^{-1} = (r_0+q\theta) \times q^{-1} = \theta - c; \qquad c = -r_0 \times q^{-1} \text{ entier rationnel.}$$

L'ensemble **I** est donc égal à un idéal, défini par sa forme canonique

$$\mathbf{I} = q \times \mathbf{M}; \qquad \begin{cases} q \text{ nombre rationnel positif;} \\ \mathbf{M} \text{ idéal canonique.} \end{cases}$$

8. 3. *Idéaux entiers.*

DÉFINITION. — *Un idéal fractionnaire* **I**, d'un corps $\mathbf{R}(\theta)$, *est appelé* **idéal entier**, *lorsque son facteur rationnel q est un nombre entier*; [en particulier si $q = 1$, c'est-à-dire si **I** est un *idéal canonique*].

Il est équivalent de dire que *tous les éléments*, de l'idéal **I**, *sont des entiers*, du corps (**3**) —ou que **I** est contenu dans l'ensemble $\mathbf{E}(\theta)$, des entiers de $\mathbf{R}(\theta)$, dont on a dit qu'il était un idéal trivial— .

La deuxième propriété est *nécessaire*: les produits par un nombre entier q, des entiers (algébriques) du facteur canonique **M** sont des entiers du corps.

Elle est *suffisante*: si l'idéal **I** ne contient que des entiers du corps, leurs facteurs rationnels et le plus petit d'entre eux sont des nombres entiers.

L'idéal trivial $\mathbf{E}(\theta)$ est ainsi l'idéal *maximum*, aussi bien des idéaux canoniques, que des idéaux entiers, en ce sens qu'il en est un et qu'il les contient tous. Il est appelé l'**idéal unité**; qualificatif qui sera, à nouveau justifié ci-dessous (**12**).

On peut aussi donner une définition axiomatique d'un *idéal entier* par des conditions directes d'appartenance à un sous ensemble du domaine des entiers $\mathbf{E}(\theta)$:

pour qu'un ensemble **I**, d'*entiers* du corps $\mathbf{R}(\theta)$, soit un idéal (nécessairement *entier*) il faut et il suffit qu'*il vérifie les conditions* 1 (module) *et* 3 (produit par tout entier du corps), des propriétés caractéristiques des idéaux (canonique, **7**, ou fractionnaire, **8**).

8. 4. *Multiplication d'un idéal par un élément.*

De la définition axiomatique d'un idéal fractionnaire, on peut déduire immédiatement des propriétés qui seront reprises ci-dessous comme cas particuliers de la multiplication des idéaux (**13**).

L'ensemble **J**, *des produits*, des éléments d'un idéal fractionnaire **I**, *par un élément* ρ, du corps, est *encore un idéal.* Cette propriété peut être exprimée par les relations réciproques; si ρ n'est pas nul:

$$\mathbf{J} = \rho \times \mathbf{I} \quad \Leftrightarrow \quad \mathbf{I} = \rho^{-1} \times \mathbf{J}; \qquad \mathbf{I}, \mathbf{J} \text{ idéaux.}$$

La forme canonique d'un idéal **I** et la construction de son facteur canonique **M**, en sont des cas particuliers:

$$\mathbf{I} = q \times \mathbf{M} \quad \Leftrightarrow \quad \mathbf{M} = q^{-1} \times \mathbf{I}; \qquad q \text{ facteur rationnel de } \mathbf{I}.$$

On peut en remarquer divers cas particuliers:

Si ρ est un élément rationnel q', non nul, les idéaux **I** et $q' \times \mathbf{I}$ ont le même facteur canonique:

$$\mathbf{I} = q \times \mathbf{M} \quad \Rightarrow \quad q' \times \mathbf{I} = (q \times |q'|) \times \mathbf{M}.$$

Le cas de $\rho = 0$ est trivial: $\quad 0 \times \mathbf{I} = 0.$

Si ρ est un entier α, du corps, *l'idéal* $\alpha \times \mathbf{I}$ *est contenu dans* **I**, car tout produit $\alpha \times$ élément de **I**, appartient à **I** (condition 3).

Si ρ est un diviseur de l'unité η, l'idéal $\eta \times \mathbf{I}$ est égal à **I**, car:

$$\eta^{-1} \times (\eta \times \mathbf{I}) = (\eta^{-1} \times \eta) \times \mathbf{I} = \mathbf{I},$$

est contenu dans $\eta \times \mathbf{I}$, qui lui-même contient **I**, de sorte qu'ils sont égaux.

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**).

10. Bases algébriques.

Pour engendrer un idéal avec certains de ses éléments, on peut conjuguer, à l'addition et à la soustraction, la multiplication par des entiers du corps; ceci conduit à la définition suivante (comparer à celle d'une base arithmétique; **9**).

DÉFINITION. — *On appelle* **base algébrique**, d'un idéal fractionnaire **I**, *un système* de *h éléments* ρ_i, de **I**, tel que *tout élément* ρ, *de* **I**, *soit égal à une forme* (linéaire) *de ces termes* ρ_i, pour des valeurs des variables —ou des *multiplicateurs*— égaux à des *entiers du corps*

$$\rho = \Sigma \xi_i \times \rho_i; \qquad i \text{ de } 1 \text{ à } h; \qquad \xi_i \text{ entiers du corps.}$$

Une *base arithmétique* d'un idéal **I** est, à fortiori algébrique: tout élément de **I** est égal à une forme, pour des multiplicateurs entiers rationnels, donc, entiers du corps.

D'autre part, la multiplication des ρ_i par des entiers du corps ne donne que des éléments de **I**.

Il n'y a pas de condition imposée aux éléments d'une base algébrique; c'est ce que précise la propriété suivante.

THÉORÈME de la génération d'un idéal par une base algébrique. — Dans un corps $\mathbf{R}(\theta)$, *étant donné* (arbitrairement) *un système*, d'un nombre fini *h* (peut être réduit à 1) *d'éléments* ρ_i, du corps, *l'ensemble des sommes*, de leurs produits par des entiers du corps;

$$\rho = \Sigma \xi_i \times \rho_i; \qquad i \text{ de } 1 \text{ à } h; \qquad \xi_i \text{ entiers du corps;}$$

est un idéal fractionnaire, dont le système des ρ_i est une *base algébrique.*

Cet idéal est désigné par la notation:

$\mathbf{I} = (\ldots,\rho_i,\ldots)$; (les ρ_i éventuellement écrits nommément); (dont on précisera, le cas échéant, qu'elle est une base arithmétique). Elle a déjà été employée pour un idéal défini par sa base canonique (qm, $q \times (\theta - c)$) (ci-dessus **7. 1** et **8. 1**).

L'ensemble des éléments ρ, ainsi construit, vérifie bien les conditions du théorème caractéristique (**8. 2**): il contient les différences (et sommes mutuelles), obtenues par les différences des multiplicateurs ξ_i, de même indice; et les produits par tout entier α, du corps, obtenus en multipliant les ξ_i par α. En outre les facteurs rationnels des éléments ρ sont limités inférieurement, au moins par le p.g.c.d. w des facteurs rationnels des termes ρ_i. Car les produits $w^{-1} \times \rho_i$, ayant des facteurs rationnels entiers, sont des entiers du corps. Alors, pour tout élément ρ:

$$\rho = w \times (\Sigma \xi_i \times (w^{-1} \times \rho_i)) = w \times \text{entier du corps};$$

son facteur rationnel est un multiple de w, donc lui est au moins égal.

A une base algébrique, *on peut*, évidemment, *adjoindre d'autres éléments de l'idéal engendré*, c'est-à-dire toute valeur d'une forme des termes de la base, pour des variables, égales à des entiers du corps.

Inversement, dans une base algébrique, définissant un idéal, *on peut* supprimer un terme, s'il est égal à une forme linéaire des autres, pour des valeurs des variables, égales à des entiers du corps.

10. 2. *Cas particuliers et opérations.*

L'*élément unité* 1 est, à lui seul, une base algébrique de l'idéal trivial $\mathbf{E}(\theta)$, qui est, par suite désigné par (1) et dont on a déjà dit qu'il était appelé *l'idéal unité* (**8. 3**), nom qui sera ci-dessous (**12**) l'objet d'une justification complémentaire. On peut adjoindre à 1 des entiers quelconques du corps et inversement *une base formée d'entiers du corps et comprenant* 1 *engendre l'idéal* (1).

Un élément unique ρ est une base algébrique de l'idéal formé par les produits de ρ par tous les entiers du corps, donc du produit par ρ de l'idéal unité (**8. 4**):

$$(\rho) = \rho \times (1), \quad \text{ou} \quad \rho \times \mathbf{E}(\theta);$$

un tel idéal est appelé **principal**, de base ρ (ci-dessous **11**).

La *multiplication* par un élément (**8. 4**) —et la *conjugaison* (**8. 5**)— d'un idéal sont réalisées par des opérations simples

sur une base algébrique (produits par ρ —et conjugués— de ses termes):

$$\rho \times (\ldots,\rho_i,\ldots) = (\ldots,\rho \times \rho_i,\ldots);$$
$$(\ldots,\rho_i,\ldots)' = (\ldots,\rho_i',\ldots).$$

La vérification est immédiate; éventuellement les bases restent arithmétiques, ce qui a déjà été constaté directement (**9. 2** et **9. 3**).

10. 3. *Propriétés d'inclusion.*

De la génération des idéaux par des bases algébriques, on déduit immédiatement des propriétés d'inclusion dont on indique ci-dessous qu'elles sont aussi des propriétés de *divisibilité* (**18 bis**).

Pour qu'*un idéal* **F** *contienne un idéal* **I**, défini par une *base algébrique*, il faut et il suffit que *chacun des termes* ρ_i *de cette base appartienne à* **F**, ou que chaque idéal principal (ρ_i) soit inclus dans **F**:

$$(\ldots,\rho_i,\ldots) \subset \mathbf{F} \quad \Leftrightarrow \quad \rho_i \in \mathbf{F} \quad [\text{ou } (\rho_i) \subset \mathbf{F}], \qquad \text{tout } i.$$

En particulier, pour qu'un idéal **I**, défini par une base algébrique soit *entier* (**8. 3**) —ou soit contenu dans l'idéal (1)— il faut et il suffit que les termes de sa base soient des entiers du corps.

La propriété d'inclusion s'étend immédiatement à plusieurs idéaux: *pour qu'un idéal* **F** *contienne des idéaux* (un ou plusieurs) définis par des bases algébriques, il faut et il suffit qu'*il contienne tous les termes des bases.*

Ceci peut être exprimé par la définition —ou construction— et la propriété suivantes.

Pour un système (d'un nombre fini) d'idéaux, définis par des bases algébriques:

$$\mathbf{I} = (\ldots,\rho_i,\ldots), \quad \mathbf{J} = (\ldots,\rho_j,\ldots), \quad \ldots$$

on appelle plus petit idéal contenant —et on appellera ci-dessous *plus grand commun diviseur*— l'idéal **D**, dont une base algébrique est constituée par la *réunion des bases*, des idéaux considérés:

$$\mathbf{D} = (\ldots,\rho_i,\ldots;\ldots,\rho_j,\ldots;\ldots), \quad \text{en abrégé } (\mathbf{I},\mathbf{J},\ldots).$$

Pour qu'un idéal **F** contienne des idéaux **I,J**,..., il faut et il suffit qu'il contienne leur plus petit idéal contenant:

$$\{\mathbf{I} \subset \mathbf{F} \quad \text{et} \quad \mathbf{J} \subset \mathbf{F}, \quad \text{et} \quad \ldots\} \Leftrightarrow (\mathbf{I},\mathbf{J},\ldots) \subset \mathbf{F}.$$

La propriété résulte immédiatement de l'énoncé précédent. Elle montre que la construction de l'idéal **D** est indépendante des bases choisies pour définir les idéaux considérés: un idéal $\mathbf{D}_1$ construit avec d'autres bases doit être contenu dans **D**, mais aussi le contenir; ils sont donc égaux.

La construction de **D** est donc une opération déterminée sur les idéaux **I,J**, ...; c'est une égalité dans le cas d'un seul idéal; elle est manifestement associative et commutative.

La notation adoptée pour un idéal défini par une base algébrique de termes ρ_i, peut être considérée comme l'indication de la construction du plus petit idéal contenant les idéaux principaux (ρ_i):

$$(\ldots,\rho_i,\ldots) = (\ldots,(\rho_i),\ldots).$$

Par analogie avec le vocabulaire de l'arithmétique élémentaire, on dit que *des idéaux principaux* (α_i), —ou leurs bases α_i— *sont* premiers entre eux, dans leur ensemble, lorsque leur plus petit idéal contenant est l'idéal unité —ou lorsque le système des bases α_i constitue une base algébrique de l'idéal unité— :

$$(\ldots,\alpha_i,\ldots) = (1).$$

On vérifie aisément qu'il en est ainsi si et seulement si les α_i sont des entiers du corps et s'il existe des entiers ξ_i, du corps tels que $\Sigma\xi_i \times \alpha_i = 1$.

Des nombres entiers, premiers entre eux, au sens de l'arithmétique ordinaire, considérés comme des entiers rationnels, d'un corps quadratique, sont aussi premiers, au sens précédent.

10. 4. *Construction d'une base arithmétique.*

En modifiant une base algébrique par remplacement, ou par adjonction de termes on peut la rendre arithmétique.

Pour un idéal **I**, défini par une base algébrique de h éléments ρ_i, *on obtient une base arithmétique*, de $2h$ éléments, *en multipliant par chaque terme* ρ_i *les deux termes* γ_1 γ_2, *d'une base arithmétique des entiers du corps* —ou de l'idéal unité— (**4**):

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

On peut choisir notamment, comme il a été fait pour le théorème caractéristique (**9. 5**), une base 1τ, des entiers. La modification de la base se borne alors à l'adjonction des h termes $\tau \times \rho_i$:

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

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 ρ_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 τ, 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* ρ; c'est-à-dire lorsqu'il est égal au produit par l'élément ρ de l'idéal unité (1).

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

$$(\rho) \quad \text{abréviation de} \quad \rho\times(1), \quad \text{ou} \quad \rho\times\mathbf{E}(\theta).$$

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 (ρ_1), (ρ_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:

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

L'implication est obtenue en multipliant les deux membres de la première égalité par l'inverse de ρ_2, supposé non nul. Les entiers ξ_1 et ξ_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 (ρ), en multipliant par ρ des bases arithmétiques de (1):

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

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 (ρ), de base ρ, élément du corps:

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

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

2. Le *facteur canonique* **M** est égal à l'idéal principal (α), dont une base α est l'*entier canonique* du corps égal au quotient de ρ 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:

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

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

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 (α) soit *entier*, il faut et il suffit que *sa base* α *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.*

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

Pour calculer une base canonique d'un idéal principal, il suffit de chercher la norme et une racine de son facteur canonique **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:

$$(a+b\theta); \quad a,b \text{ (nombres entiers) premiers entre eux;}$$

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 α:

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

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 (α):

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

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 le valeur de c par le calcul:

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

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:

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

(A suivre)