7. Idéaux canoniques.

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:

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