24. Congruence d'idéaux canoniques.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **6 (1960)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

24. Congruence d'idéaux canoniques.

La congruence des idéaux et la formation des classes peuvent être ramenées *à une congruence et à un calcul d'idéaux canoniques*, en utilisant la remarque suivante:

Un idéal fractionnaire $\mathbf{I} = q \times \mathbf{M}$ *est congru à son facteur canonique* $\mathbf{M}$.

La forme canonique d'un idéal $\mathbf{I}$ (**8**) est en effet le produit de son facteur canonique $\mathbf{M}$ par le facteur rationnel q, —ou l'idéal principal (rationnel) (q)— (**12**).

Donc deux idéaux, non nuls, sont congrus, si et seulement si il en est ainsi de leurs facteurs canoniques (puisque la congruence est transitive).

Ces considérations sont encore des conséquences des *propriétés générales des groupes*. Le groupe $\mathcal{R}$, des idéaux principaux admet comme sous-groupe, le groupe $\mathfrak{Q}$ des idéaux principaux rationnels. Dans chaque classe de $\mathcal{G}$ et de $\mathcal{R}$, mod. $\mathfrak{Q}$, il y a un et un seul idéal canonique. La répartition des idéaux canoniques en classes est donc équivalente à la formation du groupe quotient des groupes quotients $(\mathcal{G}|\mathfrak{Q})|(\mathcal{R}|\mathfrak{Q})$.

La relation d'*association* (**16**) d'idéaux canoniques, qui se présente naturellement, comme il a été dit (**21**), dans l'*algorithme du tableau de valeurs*, entraîne une relation entre les classes.

Théorème des idéaux associés. — *Deux idéaux canoniques associés*, relativement à une racine c, *définissent* —ou engendrent— *des classes inverses*, donc conjuguées (**23**). En particulier un *idéal réfléchi* définit une *classe double* (**23**).

En effet, le produit de deux idéaux associés, suivant une racine c, étant l'idéal principal $(\theta - c)$, le produit des classes qu'ils définissent est la classe principale —ou chacun est congru à l'idéal conjugué de l'autre— :

$$\mathbf{M} \times \mathbf{N} = (\theta - c) \quad \Rightarrow \quad \mathbf{M} \sim \mathbf{N}' \quad \text{et} \quad \mathbf{M}' \sim \mathbf{N}.$$

On peut expliciter cette relation de congruence en précisant une base de l'idéal principal multiplicateur. Les expressions:

$$\mathbf{M} = (m, \ \theta - c), \quad \mathbf{N} = (n, \ \theta - c); \quad m \times n = |F(c)|;$$

entraînent:

$$\mathbf{M}\times[(\theta'-c):m] = \mathbf{N}'; \qquad \mathbf{M} = \mathbf{N}'\times[(\theta-c):n].$$

En appliquant la règle du produit d'idéaux, définis l'un par une *base arithmétique*, l'autre par une *base algébrique* (**13**), on obtient:

$$\begin{aligned}\mathbf{M}\times(\theta'-c) &= (m, \theta-c)\times(\theta'-c) = (m\times(\theta'-c),\ (\theta-c)\times(\theta'-c))\\ &= (m\times(\theta'-c), F(c)) = (m\times(\theta'-c), m\times n) = (m)\times\mathbf{N}'.\end{aligned}$$

On peut vérifier de même la seconde formule; on peut aussi bien former le produit des deux multiplicateurs indiqués qui doivent être inverses:

$$\begin{aligned}&[(\theta'-c):m]\times[(\theta-c):n] =\\ &\qquad [(\theta'-c)\times(\theta-c)]:(m\times n) = [F(c)]:(m\times n);\end{aligned}$$

le résultat est bien égal à $+1$ ou à -1 (suivant le signe de $F(c)$).

La congruence de deux idéaux canoniques établit entre leurs éléments une correspondance biunivoque qui conserve l'addition —ou est un *isomorphisme des modules*— . Elle fait par suite corespondre des bases arithmétiques libres (**9**).

Théorème des bases des idéaux congrus. — *Une congruence entre des idéaux canoniques* **M** *et* $\mathbf{M}_1$, *fait correspondre à une base arithmétique libre*, de l'un $\mathbf{M}_1$ (qui peut être sa base canonique), *une base arithmétique libre de l'autre* **M** (donc équivalente arithmétiquement à sa base canonique (**9**).

Les éléments ξ, de l'idéal canonique $\mathbf{M}_1$, sont des entiers algébriques, représentés proprement, au moyen d'une base arithmétique libre de deux éléments $\alpha_1\ \beta_1$ par les expressions:

$$\xi = x\times\alpha_1 + y\times\beta_1; \qquad x,y \text{ entiers rationnels.}$$

La congruence étant définie par un multiplicateur (élément du corps) ρ, non nul, les produits:

$$\rho\times\xi = \rho\times(x\times\alpha_1+y\times\beta_1) = x\times(\rho\times\alpha_1)+y\times(\rho\times\beta_1),$$

sont des éléments de $\mathbf{M} = \rho\mathbf{M}_1$, donc des entiers algébriques, qui sont représentés ainsi au moyen de la *base arithmétique* $\rho\times\alpha_1\ \rho\times\beta_1$. Cette représentation est propre et la *base est libre*, car l'annulation de $\rho\times\xi$ est équivalente à celle de ξ; donc à celle de x et de y.

En outre les éléments de $\mathbf{M}$ et de $\mathbf{M}_1$ se correspondent, en étant *représentés par les mêmes coefficients* (entiers rationnels) relativement aux bases correspondantes, $\alpha_1\ \beta_1$ et $\rho\times\alpha_1\ \rho\times\beta_1$.

Cette correspondance peut notamment être appliquée à des idéaux congrus, construits par l'intermédiaire d'idéaux associés:

$$\mathbf{M} = (m,\ \theta-c), \quad \mathbf{N} = (n,\ \theta-c); \quad \mathbf{M}_1 = \mathbf{N}'.$$

La congruence de $\mathbf{M}_1$ à $\mathbf{M}$ est réalisée par le multiplicateur $(\theta-c): n$. Appliqué à la base $(n,\ \theta'-c)$, de $\mathbf{M}_1$ il donnerait la base canonique de $\mathbf{M}$. Mais, appliqué à une base $(n,\ \theta-c_1)$, (où c_1 est une racine conjuguée de c, suivant le module n), il donne une base arithmétique libre de $\mathbf{M}_1$:

$$n\times[(\theta-c): n] = (\theta-c), \quad [(\theta-c_1)\times(\theta-c)]: n$$

qui peut être différente de la base canonique, mais lui est arithmétiquement équivalente.

Dans l'exemple du tableau I, on peut considérer les idéaux associés:

$$\mathbf{M} = (3,\ \theta-1), \quad \mathbf{N} = (4,\ \theta-1), \quad \mathbf{M}_1 = \mathbf{N}' = (4,\ \theta-2);$$

le multiplicateur de $\mathbf{M}_1$ étant $(\theta-1): 4$, à la base choisie de $\mathbf{M}_1$, il fait correspondre:

$$4\times[(\theta-1): 4] = \theta-1, \quad [(\theta-1)\times(\theta-2)]: 4 = -\theta-2.$$

On vérifie bien que ce couple d'éléments est bien arithmétiquement équivalent à la base canonique de $\mathbf{M}$:

$$\begin{Vmatrix} \theta-1 \\ -\theta-2 \end{Vmatrix} = \begin{Vmatrix} 0 & 1 \\ -1 & -1 \end{Vmatrix} \times \begin{Vmatrix} 3 \\ \theta-1 \end{Vmatrix}$$

25. Idéaux canoniques réduits.

THÉORÈME du nombre de classes d'idéaux. — Dans un corps quadratique, *le nombre de classes d'idéaux*, (mod. $\mathcal{R}$) —ou l'ordre du groupe quotient $\mathcal{G}|\mathcal{R}$— *est fini.*