BULLETIN DE LA S. M. F.

T. LALESCO

Sur la représentation des nombres par les classes de formes appartenant à un déterminant donné

Bulletin de la S. M. F., tome 35 (1907), p. 248-252
<http://www.numdam.org/item?id=BSMF_1907__35__248_0>

SUR LA REPRÉSENTATION DES NOMBRES PAR LES CLASSES DE FORMES APPARTENANT A UN DÉTERMINANT DONNÉ;

PAR M. T. LALESCO.

1. Dans l'étude de la représentation des nombres par les classes de formes appartenant à un déterminant donné D, on peut se borner à considérer le groupe des classes primitives, c'est-à-dire des classes de formes

$$ax^2 + 2bxy + cy^2, \tag{1}$$

les nombres a, b et c étant premiers dans leur ensemble.

On sait que la véritable représentation d'un nombre m par une forme (1) est celle que l'on appelle la représentation *propre* de ce nombre, c'est-à-dire une représentation telle que

$$m = a\xi^2 + 2b\xi\eta + c\eta^2,$$

où les nombres ξ et η sont premiers entre eux, car les représentations impropres reviennent toujours à des représentations propres irréductibles.

Ceci rappelé, prenons deux nombres m et n représentés proprement par deux classes quelconques que nous désignerons par K_m et K_n. La théorie de la composition des formes nous apprend alors que le produit mn pourra être représenté par la classe composée que nous désignerons par $K_m K_n$; mais cette représentation sera-t-elle propre ou non?

Si les nombres m et n sont premiers entre eux, une identité fondamentale de la théorie de la composition des formes montre tout de suite que cette représentation résultante sera propre également; mais, si les nombres m et n ne sont pas premiers entre eux, cela n'est plus vrai, comme on l'a admis quelquefois. Je me propose de montrer ici qu'en général, dans ce cas, il y a plus de représentations résultantes impropres et j'établirai un critère permettant de distinguer les deux cas.

2. Soient

$$m = a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k} b_1^{\beta_1} b_2^{\beta_2} \ldots b_p^{\beta_p},$$
$$n = a_1^{\alpha'_1} a_2^{\alpha'_2} \ldots a_k^{\alpha'_k} c_1^{\gamma_1} c_2^{\gamma_2} \ldots c_q^{\gamma_q},$$

les deux nombres considérés, supposés d'abord premiers à $2D$. Faisons la remarque évidente que toute représentation propre d'un produit de deux facteurs premiers entre eux provient nécessairement de la composition de deux représentations propres convenables de ses facteurs; en effet, l'identité fondamentale

$$aa'X^2 + 2bXY + cY^2 = (ax^2 + 2bxy + a'cy^2)(a'x'^2 + 2bx'y' + acy'^2),$$

où

$$X = xx' - cyy',$$
$$Y = ax'y + a'xy' + 2byy',$$

nous montre que la représentation propre du nombre aa' par la forme (aa', b, c) peut résulter de la composition des représentations propres des nombres a et a' à l'aide des formes $(a, b, a'c)$ et (a', b, ac).

Pour former donc toutes les représentations propres d'un nombre composé, il suffira de déterminer toutes les représentations propres de ses facteurs premiers deux à deux et de composer ensuite ces représentations de toutes les manières possibles. Or, soit K_λ et K_λ^{-1} les deux classes opposées qui, elles seules, représentent proprement le nombre premier λ; la puissance λ^n ne sera représentable proprement que par les classes K_λ^n et K_λ^{-n}, en représentant par K_λ^n la classe qui résulte de la composition de K_λ, n fois de suite avec elle-même. Comme, d'après une remarque déjà faite, les représentations propres de deux nombres premiers entre eux donnent par composition une représentation qui est propre aussi, les expressions générales des classes dont chacune fournira une représentation propre distincte des nombres m et n seront respectivement

$$K_m = K_{a_1}^{\pm\alpha_1} K_{a_2}^{\pm\alpha_2} \ldots K_{a_k}^{\pm\alpha_k} K_{b_1}^{\pm\beta_1} \ldots K_{b_p}^{\pm\beta_p},$$
$$K_n = K_{a_1}^{\pm\alpha'_1} K_{a_2}^{\pm\alpha'_2} \ldots K_{a_k}^{\pm\alpha'_k} K_{c_1}^{\pm\gamma_1} \ldots K_{c_q}^{\pm\gamma_q}.$$

Nous obtenons ainsi 2^{p+k} représentations propres différentes du nombre m et 2^{q+k} du nombre n.

Considérons maintenant le produit

$$mn = a_1^{\alpha_1+\alpha'_1} \dots a_k^{\alpha_k+\alpha'_k} b_1^{\beta_1} \dots b_p^{\beta_p} c_1^{\gamma_1} \dots c_q^{\gamma_q}.$$

Ce nombre aura donc effectivement et seulement 2^{p+q+k} représentations propres par les classes du déterminant D. Or, on peut combiner une représentation propre du nombre m à une représentation propre de n, de 2^{p+q+2k} façons différentes. *Il y aura donc, en général,* $2^{p+q+k}(2^k - 1)$ *cas où la représentation résultante du produit mn ne sera pas propre, quoique les représentations des nombres m et n le soient.*

Si donc $k > 1$, c'est le nombre des cas d'exception qui sera le plus grand. D'autre part, il est évident que les représentations impropres seront données par les classes

$$\mathrm{K}_{a_1}^{\pm(\alpha-\alpha')} \dots \mathrm{K}_{a_k}^{\pm(\alpha_k-\alpha'_k)} \mathrm{K}_{b_1}^{\pm\beta_1} \dots \mathrm{K}_{b_p}^{\pm\beta_p} \mathrm{K}_{c_1}^{\pm\gamma_1} \dots \mathrm{K}_{c_q}^{\pm\gamma_q},$$

et ceci nous permet d'énoncer le résultat suivant :

La représentation résultante sera impropre toutes les fois que, dans les représentations propres des nombres m et n, l'un au moins des facteurs communs de ces nombres sera représenté par des classes opposées, et seulement dans ce cas.

3. Examinons maintenant les représentations des nombres qui ne sont pas premiers à 2D.

D'après la remarque faite plus haut, cette question revient à l'étude de la représentation du nombre 2 et des facteurs de D. Nous supposerons ici D *sans diviseurs carrés;* dans ces conditions, je dis qu'on a le théorème suivant :

Un facteur d de D (D $= d\delta$) *n'est représentable proprement que par la classe ambiguë*

$$dx^2 - \delta y^2.$$

Aucune puissance de ce nombre n'est représentable proprement par les classes des formes du déterminant D.

En effet, si d est représentable proprement par une classe K_d, cette classe contiendra la forme (d, n, l) où $n^2 - dl = \mathrm{D} = d\delta$:

on déduit de là $n = kd$ et, par conséquent,

$$dx^2 + 2nxy + ly^2 = d(x + ky)^2 - \delta y^2,$$

ce qui prouve que la classe K_d est bien une classe de formes ambiguës.

Prenons maintenant le nombre d^k; on devrait avoir d'une façon analogue $n^2 - d^k l = d\delta$; or, cette égalité est impossible si $k > 1$, puisque δ est premier à d.

Nous avons ainsi (remarquons-le en passant) une propriété caractéristique des formes ambiguës : ce sont les seules classes qui représentent proprement les facteurs de D. Cette propriété ne subsiste plus si D a des facteurs carrés : ainsi, par exemple, la forme $9x^2 + 6xy + 11y^2$ représente proprement $9 (x = 1, y = 0)$; son déterminant est $-90 = -3^2.10$, et pourtant ce n'est pas une forme ambiguë.

La limitation aux déterminants sans diviseurs carrés est donc utile pour simplifier les résultats, même dans la théorie de la représentation des nombres. Ce théorème s'applique aussi pour le facteur 2 si D est pair.

Il nous reste donc à examiner le cas de la représentation de 2 quand D est impair. Or, un théorème bien connu sur les congruences

$$x^2 \equiv D (\bmod 2^k)$$

nous permet d'affirmer immédiatement que 2 est toujours représentable proprement par la seule classe

$$2x^2 + 2xy + ky^2 \qquad (1 - 2k = D);$$

que 4 est toujours représentable par les deux classes opposées

$$4x^2 \pm 2xy + k'y^2 \qquad (1 - 4k' = D),$$

si D est de la forme $4n + 1$ et seulement dans ce cas, et qu'enfin $2^k (k > 2)$ est représenté proprement par 4 classes, deux à deux opposées, si $D = 8n + 1$ et seulement dans ce cas.

On voit maintenant avec facilité comment on devra modifier l'énoncé général trouvé précédemment pour ces divers cas. Ainsi, par exemple, nous aurons les propriétés suivantes :

Si un facteur de D figure à la fois dans m et n, la représen-

tation composée sera sûrement impropre ; mais, si les nombres m et n, tout en n'étant pas premiers à D, *ne sont pas divisibles par les mêmes facteurs de* D, *et si les autres conditions sont remplies, la représentation résultante sera propre.*

Dans l'évaluation des nombres p et q, il ne faudra pas tenir compte des facteurs de D ; enfin, 2 rentre dans la règle générale si D est pair.