NOUVELLES ANNALES DE MATHÉMATIQUES

T. LALESCO

Sur la composition des formes quadratiques

Nouvelles annales de mathématiques 4^e série, tome 7 (1907), p. 145-150

<http://www.numdam.org/item?id=NAM_1907_4_7__145_0>

[120a]

SUR LA COMPOSITION DES FORMES QUADRATIQUES;

PAR M. T. LALESCO.

1. Je désignerai dans cette Note par

$$(a, b, c)$$

la forme quadratique binaire à coefficients entiers

$$ax^2 + bxy + cy^2.$$

Le déterminant de cette forme est $D = b^2 - 4ac$.

La théorie de la *composition* des formes quadratiques binaires repose sur quelques principes que je rappellerai tout d'abord.

Soient (a_1, b_1, c_1), (a_2, b_2, c_2) deux formes de même déterminant D; on dit qu'elles sont *composables* si les nombres a_1, a_2 et $\frac{b_2 + b_1}{2}$ sont premiers dans leur ensemble. On peut, dans ce cas, trouver d'une infinité de manières deux entiers B et C tels que

$$(a_1, b_1, c_1) \asymp (a_1, B, a_2 C) \quad \text{et} \quad (a_2, b_2, c_2) \asymp (a_2, B, a_1 C),$$

le signe $\asymp$ désignant l'équivalence de deux formes.

Le nombre B satisfait visiblement aux congruences

$$B \equiv b_1 \pmod{2a_1}, \quad B \equiv b_2 \pmod{2a_2}, \quad B^2 \equiv D \pmod{4a_1 a_2}.$$

Les formes $(a_1, B, a_2 C)$ et $(a_2, B, a_1 C)$, telles que le dernier coefficient de chacune soit divisible par le premier coefficient de l'autre, sont dites *immédiatement composables,* et la forme

$$(a_1, a_2, BC)$$

est dite *leur forme composée*. C'est aussi *une* forme composée des deux formes initiales (a_1, b_1, c_1) et (a_2, b_2, c_2). Toutes les formes composées de deux formes composables sont équivalentes entre elles.

L'intérêt de ces considérations résulte du fait que, si deux nombres sont représentables respectivement par les formes (a_1, b_1, c_1) et (a_2, b_2, c_2), leur produit est représentable par la forme composée (a_1, a_2, BC). Cela résulte d'une identité due à Gauss, et qui généralise l'identité suivante de Lagrange :

$$(x^2 + \mathrm{A}y^2)(x'^2 + \mathrm{A}y'^2) = (xx' + \mathrm{A}yy')^2 + \mathrm{A}(xy' - z'y)^2.$$

Pour toutes ces généralités, je renvoie le lecteur au X^e^ Supplément des *Vorlesungen über Zahlentheorie* de Dirichlet-Dedekind. La terminologie dont il est fait usage ici est empruntée au Cours professé au Collège de France en 1906-1907 par M. G. Humbert sur les applications de l'Analyse à la Théorie des nombres.

2. Le théorème fondamental de la théorie de la composition est le suivant :

Toutes les formes composables qui sont respectivement équivalentes à deux formes fixes ont pour composées des formes équivalentes à une forme fixe.

La démonstration de cette proposition, telle qu'on la présente d'ordinaire, exige des calculs longs et fastidieux. Le but de cette Note est de montrer qu'on peut l'établir simplement en s'appuyant sur le lemme suivant :

Deux formes (a_1, b_1, c_1) et (a_2, b_2, c_2) composables et qui sont équivalentes jouissent de la propriété caractéristique suivante :

Il existe deux entiers x et y qui satisfont à la fois aux conditions

$$(1)\qquad \begin{cases} x^2 - Dy^2 = 4a_1a_2, \\ x + b_1y \equiv 0 \pmod{2a_1}, \\ x - b_2y \equiv 0 \pmod{2a_2}, \end{cases}$$

D *étant le déterminant commun des deux formes.*

Mettons en effet les deux formes sous la forme immédiatement composable et écrivons qu'elles sont équivalentes; nous obtenons

$$(2)\qquad \begin{cases} a_1 = a_2\alpha^2 + B\alpha\gamma + a_1C\gamma^2, \\ B = 2a_2\alpha\beta + B(\alpha\delta + \beta\gamma) + 2a_1C\gamma\delta, \\ a_2C = a_2\beta^2 + B\beta\delta + a_1C\delta^2, \end{cases}$$

où α, β, γ et δ sont des entiers satisfaisant à la relation

$$(3)\qquad \alpha\delta - \beta\gamma = 1.$$

Multiplions la première égalité par β, la seconde par α et retranchons; nous obtenons, en tenant compte de (3), la relation

$$(4)\qquad C\gamma + \beta = 0$$

et celle-ci réduit les trois égalités (2) à la relation unique

$$(5)\qquad a_2\alpha + B\gamma - a_1\delta = 0,$$

et (3) à

$$(6)\qquad \alpha\delta + C\gamma^2 = 1.$$

Des égalités (5) et (6) on déduit

$$(7)\qquad \begin{cases} 2a_1\delta = \quad B\gamma \pm \sqrt{4a_1a_2 + D\gamma^2}, \\ 2a_2\alpha = -B\gamma \pm \sqrt{4a_1a_2 + D\gamma^2}, \end{cases}$$

les signes se correspondant dans ces formules. On a

donc, puisque α et δ sont entiers, et en posant $u = \pm\sqrt{4a_1a_2 + D\gamma^2}$,

$$(8)\qquad \begin{cases} 4a_1a_2 + D\gamma^2 = u^2, \\ B\gamma + u \equiv 0 \pmod{2a_1}, \\ -B\gamma + u \equiv 0 \pmod{2a_2}. \end{cases}$$

Les relations (1) sont ainsi établies, car on a, comme il est bien connu :

$$(9)\quad B \equiv b_1 \pmod{2a_1} \qquad \text{et} \qquad B \equiv b_2 \pmod{2a_2}.$$

Réciproquement, prenons deux formes (a_1, b_1, c_1) et (a_2, b_2, c_2) composables et de même déterminant D, et supposons les relations (1) vérifiées pour des valeurs entières de x et y. Les formes étant composables, nous pourrons déterminer le nombre B de manière à satisfaire aux congruences (9); les relations (1) entraînent alors les relations (8). Les congruences (8) écrites comme égalités reviennent à (7) et celles-ci par soustraction et multiplication nous donnent les relations (5) et (6); si maintenant nous déterminons β par la relation (4), on en déduira les relations (2), ce qui prouve bien que les (a_1, b_1, c_1) et (a_2, b_2, c_2) sont équivalentes.

3. Le théorème fondamental de la composition des formes s'en déduit facilement.

Soient (a_1, b_1, c_1) et (m_1, n_1, l_1) deux formes d'une classe K_1, et (a_2, b_2, c_2) et (m_2, n_2, l_2) deux formes d'une classe K_2, les classes K_1 et K_2 étant primitives.

Supposons les formes (a_1, b_1, c_1) et (a_2, b_2, c_2) composables et soit (a_1, a_2, B, C) la forme composée et de même soit (m_1, m_2, N, L) la forme composée de (m_1, n_1, l_1) et (m_2, n_2, l_2). Il s'agit de démontrer

que les deux formes (a_1, a_2, B, C) *et* (m_1, m_2, N, L) *sont aussi équivalentes.*

On peut d'abord supposer les nombres a_1 *et* a_2 *premiers à* m_1 *et* m_2. En effet, puisque les classes K_1 et K_2 sont primitives, on pourra déterminer dans la première classe une forme $(\alpha_1, \beta_1, \gamma_1)$ et dans la seconde classe la forme $(\alpha_2, \beta_2, \gamma_2)$ de manière que α_1 et α_2 soient premiers entre eux et premiers aux nombres a_1, a_2, m_1, m_2, et il suffira évidemment de démontrer que la composée de ce dernier couple appartient à la même classe que chacune des deux formes composées que nous avons considérées.

Dans ces conditions, les formes (a_1, b_1, c_1) et (m_1, n_1, l_1) sont donc composables et équivalentes, ainsi que les formes (a_2, b_2, c_2) et (m_2, n_2, l_2); nous aurons donc les relations

$$(\alpha)\quad \begin{cases} x_1^2 - Dy_1^2 = 4a_1m_1, & x_2^2 - Dy_2^2 = 4a_2m_2, \\ x_1 + b_1y_1 \equiv 0 \pmod{2a_1}, & x_2 + b_2y_2 \equiv 0 \pmod{2a_2}, \\ x_1 - n_1y_1 \equiv 0 \pmod{2m_1}, & x_2 - n_2y_2 \equiv 0 \pmod{2m_2}. \end{cases}$$

D'autre part, les formes composées (a_1, a_2, B, C) et (m_1, m_2, N, L) sont aussi composables, puisque les nombres a_1a_2 et m_1m_2 sont premiers entre eux. Donc, d'après la réciproque du théorème précédent, ces formes seront équivalentes si les relations

$$(\beta)\quad \begin{cases} X^2 - DY^2 = 4a_1a_2m_1m_2, \\ X + BY \equiv 0 \pmod{2a_1a_2}, \\ X - NY \equiv 0 \pmod{2m_1m_2} \end{cases}$$

sont satisfaites pour des valeurs entières de X et Y. Or, en multipliant les deux égalités (α), on obtient

$$\left(\frac{x_1x_2 + Dy_1y_2}{2}\right)^2 - D\left(\frac{x_2y_1 + y_2x_1}{2}\right)^2 = 4a_1a_2m_1m_2.$$

Les expressions

$$X = \frac{x_1 x_2 + D y_1 y_2}{2}$$

et

$$Y = \frac{x_1 y_2 + x_2 y_1}{2}$$

sont des nombres entiers ainsi que cela résulte immédiatement des égalités (α).

Démontrons que ces valeurs satisfont aussi aux congruences (β). La première congruence s'écrira successivement

$$\begin{aligned} &x_1 x_2 + D y_1 y_2 + B(x_1 y_1 + y_2 x_1) \equiv 0 \pmod{4 a_1 a_2}, \\ &x_1(x_2 + B y_2) + y_1(B x_2 + D y_2) \equiv 0 \pmod{4 a_1 a_2}, \end{aligned}$$

ou, puisque $B^2 \equiv D \pmod{4 a_1 a_2}$,

$$(x_1 + B y_1)(x_2 + B y_2) \equiv 0 \pmod{4 a_1 a_2},$$

et cette congruence est évidente, d'après les congruences (α).

On vérifie tout aussi aisément le seconde congruence; on aura

$$\begin{aligned} &x_1 x_2 + D y_1 y_2 - N(x_2 y_1 + y_2 x_1) \equiv 0 \pmod{4 m_1 m_2}, \\ &x_2(x_1 - N y_1) - y_2(N x_1 - D y_1) \equiv 0 \pmod{4 m_1 m_2}, \end{aligned}$$

et, puisque $N^2 \equiv D \pmod{4 m_1 m_2}$,

$$(x_1 - N y_1)(x_2 - N y_2) \equiv 0 \pmod{4 m_1 m_2}$$

qui résulte de la multiplication des dernières congruences (α). Le théorème est ainsi complètement établi.