JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

G. LEJEUNE-DIRICHLET

De la composition des formes binaires du second degré

Journal de mathématiques pures et appliquées 2^e série, tome 4 (1859), p. 389-398.
<http://www.numdam.org/item?id=JMPA_1859_2_4__389_0>

DE

LA COMPOSITION DES FORMES BINAIRES DU SECOND DEGRÉ[*];

PAR M. G. LEJEUNE-DIRICHLET.

M'étant proposé, il y a déjà plusieurs années, la détermination du nombre de classes des formes binaires du second degré, qui répondent à un même déterminant, et voulant l'étendre à la théorie des nombres complexes, j'ai dû reprendre entièrement les éléments de la théorie des formes, qui n'avaient été développés que pour le cas des nombres entiers réels. J'ai réussi à présenter complétement en peu de pages les éléments de cette théorie, en me servant de considérations non encore employées, et qui s'appliquent aussi bien aux entiers complexes qu'aux entiers réels [**].

[*] Ce Mémoire se trouve dans le t. XLVII du Journal de Crelle. Voici le titre exact, un peu altéré dans la traduction :

De formarum binariarum secundi gradus compositione, auct. G. LEJEUNE-DIRICHLET, *commentatio mense Maio an.* 1851 *ad actum quemdam academicum in Univ. Litterarum reg. Berol. celebrandum, typis expressa et distributa.*

J'ai cru devoir traduire littéralement un Mémoire qui, comme les autres du même auteur, a le mérite assez rare de contenir ce qui est nécessaire et rien de plus. Seulement pour quelques lecteurs j'ai cité, entre crochets [*D. A.*, n° 154 et autres], les numéros des *Disquisitiones Arithmeticæ* qui contiennent les démonstrations de quelques propositions invoquées par l'auteur. Pour d'autres lecteurs plus au courant de la science des nombres, et qui voudraient seulement parcourir le Mémoire, j'ai rendu sensibles, par l'emploi des caractères *italiques*, les énoncés des diverses propositions qui le composent. Autrement le mode de rédaction aurait rendu nécessaire une lecture complète du Mémoire, pour bien mettre en évidence sa clarté et sa simplicité vraiment remarquables, surtout si on le compare à ce que l'on trouve exposé sur ce sujet dans la seconde partie de la section cinquième des *Recherches arithmétiques*.

V.-A. LEBESGUE.

[**] *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes.* (Journal de Crelle, t. XXIV.)

Dans cette recherche, je me suis borné à l'étude des propriétés qui concernent l'équivalence des formes, leur transformation et la représentation des nombres, car elles suffisaient pour la question à laquelle le Mémoire était consacré. Je n'ai point traité alors la question de la composition des formes, sujet développé par l'illustre Gauss dans la section cinquième de ses *Recherches arithmétiques* avec la plus grande généralité, mais, il est vrai, au moyen de calculs si prolixes, que très-peu de géomètres ont pu bien comprendre la nature de la composition, d'autant plus que le grand géomètre, comme il le dit lui-même, a, pour plus de brièveté, donné des démonstrations synthétiques des théorèmes les plus difficiles, en supprimant l'analyse qui les lui avait fournis. C'est pourquoi je crois pouvoir espérer qu'une exposition nouvelle et toute élémentaire de ce sujet plaira à ceux qui cultivent l'analyse.

I.

Un petit nombre de résultats connus, ou qui se tirent facilement de théorèmes connus, doivent précéder la composition des formes.

Nous dirons que les valeurs $\zeta, \zeta', \zeta'', \ldots$ *qui satisfont à la congruence*

$$u^2 \equiv D,$$

suivant les modules respectifs $m, m', m'', \ldots$ *s'accordent, ou sont concordantes, si l'on peut trouver une racine* Z *de la même congruence pour le module* $mm'm''\ldots$, *de sorte qu'on ait*

$$\zeta \equiv Z \,(\text{mod. } m), \quad \zeta' \equiv Z \,(\text{mod. } m'), \quad \zeta'' = Z \,(\text{mod. } m''), \ldots$$

Il suffira de considérer le cas de $m, m', m'', \ldots$ impairs et premiers à D.

On voit facilement qu'on ne peut satisfaire aux congruences proposées qu'autant que, relativement à chacun des nombres premiers qui divisent deux ou plusieurs des nombres $m, m', m'', \ldots$, les valeurs correspondantes $\zeta, \zeta', \zeta'', \ldots$ sont des nombres congrus entre eux. Si cette condition a lieu, on déduira des valeurs $\zeta, \zeta', \zeta'', \ldots$ les résidus $\pi, \pi', \pi'', \ldots$ de Z relativement à chacun des nombres premiers inégaux $p, p', p'', \ldots$ qui divisent le produit $mm'm''\ldots$; or ces résidus $\pi, \pi', \pi'', \ldots$ sont évidemment les racines de notre congruence suivant les modules

p, p', p'',... respectivement : il résultera donc des principes connus de la doctrine des congruences, qu'il existe une racine Z, et une seule, satisfaisant à la congruence pour le module $mm'm''$..., et l'on voit sans difficulté que l'on a

$$Z \equiv \zeta \,(\text{mod. } m), \quad Z \equiv \zeta' \,(\text{mod. } m'), \quad Z \equiv \zeta'' \,(\text{mod. } m''), \ldots.$$

Comme le terme constant D conservera toujours la même valeur dans ce qui suit, nous désignerons, pour abréger, la racine ζ, répondant au module m, par la notation (m, ζ). Au moyen de cette notation, la racine Z, qui se déduit, de la manière indiquée, des racines ζ, ζ',... sera dite *composée* de ces racines, et sera commodément désignée comme il suit :

$$(m, \zeta)(m', \zeta')(m'', \zeta'')\ldots = (mm'm''\ldots, Z).$$

Remarquons, au reste, que les racines ζ, ζ', ζ'',... sont toujours concordantes quand les nombres m, m', m'',... sont premiers entre eux, et que cela subsiste même dans le cas, ici exclu, où m, m',... ne seraient pas premiers à 2D. Il est clair, en effet, que les congruences

$$Z \equiv \zeta \,(\text{mod. } m), \quad Z \equiv \zeta' \,(\text{mod. } m'), \ldots$$

déterminent alors complétement la valeur de Z pour le module $mm'm''$,..., et que l'on a

$$Z^2 \equiv D \,(\text{mod. } mm'm''\ldots).$$

II.

Dans les formes du second degré que l'on considère ici

$$ax^2 + 2bxy + cy^2,$$

le déterminant est $D = b^2 - ac$, les coefficients a, b, c sont des entiers sans diviseur commun, tous les cas se ramenant à celui-là. On sait que les formes qui satisfont à cette condition constituent deux ordres : le premier, quand l'un au moins des coefficients extrêmes a, c est impair; le second, quand ces coefficients sont tous deux pairs. Ce second cas sera omis pour abréger, car les raisonnements qui s'appli-

quent au premier, s'appliquent aussi au second avec les modifications convenables.

Si dans la forme on donne aux indéterminées x, y des valeurs premières entre elles (ce qui sera toujours sous-entendu), de sorte qu'on ait

$$ax^2 + 2bxy + cy^2 = m,$$

le nombre m (qu'il faut toujours supposer premier à $2D$), sera dit être *représenté* par la forme.

Les nombres ξ, η étant pris tels que l'on ait $x\eta - y\xi = 1$, on sait qu'il est facile de démontrer [*D. A.*, n° 154] que l'expression

$$\zeta = (ax + by)\xi + (bx + cy)\eta$$

est racine de la congruence

$$u^2 \equiv D \pmod{m},$$

et que l'on trouve toujours la même racine, quelle que soit la manière dont varient ξ et η. Nous dirons que la racine (m, ζ) appartient à cette représentation du nombre m.

On peut encore définir cette racine d'une manière plus convenable à notre but.

Si l'équation qui donne ζ est multipliée par y, en mettant $x\eta - 1$ au lieu de $y\xi$, on trouve

$$ax + by \equiv -y\zeta \pmod{m} : \tag{1}$$

cette congruence détermine complétement ζ, pourvu que y soit premier à m.

Mais si y et m ont un commun diviseur maximum δ plus grand que l'unité, il divisera aussi a, et notre congruence (1) n'apprendra rien de plus que celle-ci

$$\frac{a}{\delta}x + b\frac{y}{\delta} \equiv -\frac{y}{\delta}\zeta \left(\text{mod.}\ \frac{m}{\delta}\right),$$

de sorte que relativement aux diviseurs de δ, s'il y en a, qui ne divi-

sent pas $\frac{m}{\delta}$, les résidus de ζ ne pourront être déterminés par la congruence; on remédie facilement à cet inconvénient, en remarquant que des équations données plus haut il résulte

$$\zeta \equiv bx\eta, \quad x\eta \equiv 1 \pmod{\delta},$$

et, par suite,

$$\zeta \equiv b \pmod{\delta}. \tag{2}$$

Cette formule, étant jointe à la précédente, on connaîtra parfaitement les résidus de ζ relativement à tous les diviseurs de m. Observons que si ε est le diviseur commun maximum des nombres x et m, on aura de même

$$\zeta \equiv -b \pmod{\varepsilon}. \tag{3}$$

A ces remarques nous joindrons les suivantes bien connues, mais qu'il sera cependant utile de trouver ici réunies.

1°. *Si deux formes sont équivalentes (proprement, ce qui sera toujours sous-entendu), et que la première se change en la seconde par le moyen de la substitution*

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

où $\alpha\delta - \beta\gamma = 1$, *tout nombre m qui peut être représenté par l'une pourra l'être aussi par l'autre* [*D. A.*, n° 166], et l'on démontre facilement que *les deux représentations liées entre elles par le moyen des équations précédentes appartiennent à la même racine* (m, ζ) [*D. A.*, n° 167]. Ainsi, les représentations qui appartiennent à l'expression donnée (m, ζ) devront être rapportées à toute une classe qui sera unique.

2°. Réciproquement, on pourra démontrer que *si les représentations du nombre m par deux formes appartiennent à la même racine* (m, ζ), *on doit en conclure l'équivalence des deux formes.* [*D. A.*, n° 168.]

3°. Enfin, il est clair que, *étant donnée une racine quelconque* (m, ζ), *il existe toujours une classe dont les formes peuvent repré-*

senter le nombre m, de sorte que la racine correspondante à ces représentations soit (m, ζ). Il est clair, en effet, que m est représenté par la forme $\left(m, \zeta, \frac{\zeta^2 - D}{m}\right)$ [*D. A.*, n° 168] dont les coefficients sont sans diviseur commun et où m est impair, en posant $x = 1, y = 0$, et que cette représentation appartient à la racine (m, ζ).

III.

Ces prémisses posées, venons à notre proposition.

Étant données les deux formes φ *et* φ' *de même déterminant* D, *soient m et m' deux nombres impairs quelconques premiers à* D, *et pouvant être représentés respectivement par les formes* φ, φ', *de manière que les racines* (m, ζ), (m', ζ') *auxquelles appartiennent ces représentations soient concordantes.* Toute la difficulté consiste à montrer que *les représentations du nombre mm' qui appartiennent à la racine* $(m, \zeta)(m', \zeta')$ *se font toujours par une même forme ou plutôt par des formes appartenant à la même classe, de quelle manière d'ailleurs que varient m et m'.* C'est là le *Théorème fondamental* de la théorie de la composition des formes.

Supposons que les formes données (a, b, c), (a', b', c') soient préparées de sorte que les expressions (a, b), (a', b') soient concordantes, ce qui arrivera, par exemple, si l'on transforme les formes en d'autres équivalentes dont les coefficients des premiers termes soient premiers entre eux. Il faut bien remarquer que l'analyse suivante suppose seulement que les expressions (a, b), (a', b') sont concordantes : il n'est pas nécessaire que a et a' soient premiers entre eux, ni même à 2 D.

En désignant par (aa', B) l'expression composée de (a, b) et (a', b'), telle qu'on ait $B \equiv b \pmod{a}$, $B \equiv b' \pmod{a'}$, $D = B^2 - aa'C$, où C est entier, il est clair que les formes φ, φ' sont équivalentes aux suivantes

$$ax^2 + 2Bxy + a'Cy^2 = \varphi,$$
$$a'x'^2 + 2Bx'y' + aCy'^2 = \varphi',$$

dans lesquelles on peut les transformer.

La première équation étant multipliée par a, la seconde par a', puis

les équations résultantes multipliées membre à membre, on trouvera les équations

$$(ax + By)^2 - Dy^2 = a\varphi,$$
$$(a'x' + By')^2 - Dy'^2 = a'\varphi',$$
$$[(ax + By)(a'x' + By') + Dyy']^2$$
$$- D[(ax + By)y' + (a'x' + By')y]^2 = aa'\varphi\varphi',$$

et si l'on observe qu'à cause de $D = B^2 - aa'C$, on a

$$(4) \qquad (ax + By)(a'x' + By') + Dyy' = aa'X + BY,$$

où l'on pose

$$(5) \quad \begin{cases} X = xx' - Cyy', \\ Y = (ax + By)y' + (a'x' + By')y = axy' + a'x'y + 2Byy', \end{cases}$$

la dernière équation, divisée par aa', prendra la forme

$$(6) \qquad aa'X^2 + 2BXY + CY^2 = \varphi\varphi' = \psi.$$

Après avoir montré que le produit des formes φ, φ' se représente indéfiniment par la forme ψ, supposons aux indéterminées x, y, et de même à x', y' premières entre elles, des valeurs déterminées desquelles il résulte $\varphi = m$, $\varphi' = m'$, et qui satisfassent aux conditions indiquées. Il restera à démontrer :

1°. Que la représentation du nombre mm' par la forme ψ, qui se tire des équations (5) et (6), est propre, c'est-dire que X et Y sont premiers entre eux ;

2°. Que la racine (mm', Z), à laquelle la représentation appartient, est en effet composée des racines (m, ζ), (m', ζ'), auxquelles appartiennent les représentations des nombres m, m'.

Premièrement. Pour montrer que X et Y n'ont pas de facteur commun, partons de cette supposition qu'un nombre premier p les divise tous les deux, et voyons ce qui en résulte. Puisque p devra diviser l'un ou l'autre des nombres m, m', supposons que m soit multiple de p. Il en résultera que m' doit être aussi supposé divisible par p. En effet, X et Y étant divisibles par p, en multipliant respectivement les équa-

tions (5) par $-ay'$ et x', en les ajoutant on obtiendra l'entier divisible par p

$$(a'x'^2 + 2Bx'y' + aCy'^2)y = m'y.$$

Si l'on ne suppose pas m' divisible par p, il faudra supposer que y et par suite a sont divisibles par p. Alors à cause de

$$xx' - Cyy' = X \equiv 0 \pmod{p},$$

x, y étant premiers entre eux, il en résultera x' divisible par p, et

$$m' = a'x'^2 + 2Bx'y' + aCy'^2$$

montrera que m' est aussi multiple de p. Le nombre p divisant les deux nombres m, m', les équations (1)

$$ax + By \equiv -y\zeta, \quad a'x' + By' \equiv -y'\zeta' \pmod{p}$$

transforment la seconde équation (5) dans la congruence

$$(\zeta + \zeta')yy' \equiv 0 \pmod{p}.$$

Si l'on avait $\zeta + \zeta' \equiv 0$, il en résulterait $\zeta \equiv -\zeta'$, contre l'hypothèse que les racines ζ et ζ' sont concordantes, ce qui donne $\zeta \equiv \zeta'$. Il ne reste donc à faire qu'une des deux suppositions $y \equiv 0$, $y' \equiv 0$, qui sont tout à fait semblables. Si l'on avait $y \equiv 0$, comme déjà $xx' - Cyy' \equiv 0$, x' serait aussi divisible par p, et nous aurions par les équations (2) et (3)

$$\zeta \equiv B, \quad \zeta' \equiv -B,$$

et par suite, comme plus haut,

$$\zeta + \zeta' \equiv 0 \pmod{p};$$

il est donc prouvé que X et Y sont premiers entre eux.

Secondement. Pour montrer maintenant que la racine (mm', Z), à laquelle appartient la représentation de mm', est en effet composée des racines (m, ζ), (m', ζ'), il suffira, à cause de la symétrie, de montrer

que l'on a $Z \equiv \zeta$ relativement à tout diviseur p premier de m. Comme on a par l'équation (1)

$$ax + By \equiv -y\zeta \pmod{p},$$

de l'équation (4) et de la seconde équation (5), on tirera facilement les congruences

$$[-\zeta(ax' + By') + Dy']y \equiv aa'X + BY,$$
$$[-\zeta y' + a'x' + By']y \equiv Y;$$

la dernière étant multipliée par ζ, et ajoutée à la première, au moyen de la congruence $\zeta^2 \equiv D$, on aurait

$$aa'X + BY \equiv -Y\zeta \pmod{p}.$$

Cette congruence étant comparée à cette autre

$$aa'X + BY \equiv -YZ \pmod{p},$$

il en résulte

$$Z \equiv \zeta \pmod{p},$$

si p ne divise pas Y.

Il reste à considérer le cas de Y divisible par p. Dans ce cas on a par l'équation (2), $Z \equiv B$. Si y est aussi multiple de p, on aura semblablement $\zeta \equiv B$, et par suite $Z \equiv \zeta$. Mais si y n'est pas divisible par p, on conclut de la congruence trouvée plus haut, que l'on a

$$a'x' + By' - \zeta y' \equiv 0;$$

d'où l'on déduit facilement que p est diviseur de $a'm'$. On a, en effet,

$$(a'x' + By')^2 - Dy'^2 \equiv (a'x' + By')^2 - \zeta^2 y'^2 \equiv 0 \pmod{p}.$$

Il faut maintenant distinguer deux cas.

Supposons d'abord que a' n'est pas divisible par p; alors m' l'est, et l'on aura

$$a'x' + By' + \zeta' y' \equiv 0,$$

formule qui, comparée avec la précédente, donne

$$(\zeta + \zeta')y' \equiv 0,$$

congruence qui conduit à une absurdité; car comme $\zeta + \zeta'$ ne peut être multiple de p, il s'ensuivrait $y' \equiv 0$, et par suite, à cause de $m' = a'x'^2 + 2Bx'y' + aCy'^2$, $a' \equiv 0$, contre l'hypothèse. Ce cas ne peut donc avoir lieu. Dans le second cas, où a' est divisible par p, de la congruence

$$a'x' + By' - \zeta y' \equiv 0,$$

on déduit

$$(B - \zeta)y' \equiv 0.$$

Si p ne divise pas y', on aura

$$\zeta \equiv B,$$

ce qui s'accorde avec la congruence

$$Z \equiv B \pmod{p}.$$

Mais si p est diviseur de y', et par suite aussi de m', on aura par l'équation (2), $\zeta' \equiv B$; d'où, comme plus haut, $\zeta \equiv B$, puisque les racines ζ et ζ' s'accordent entre elles.