JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

EISENSTEIN

Extrait d'une lettre adressé à M. Charles Hermite

Journal de mathématiques pures et appliquées 1re série, tome 17 (1852), p. 473-477.

<http://www.numdam.org/item?id=JMPA_1852_1_17__473_0>

Extrait d'une Lettre adressée à M. CHARLES HERMITE,
par M. EISENSTEIN.

Dans la communication que vous me faites sur les formes ternaires, etc., vous vous êtes extrêmement approché d'une théorie que j'ai imaginée pour la comparaison des formes de déterminants *quelconques différents*, et à laquelle je vous ai déjà fait une légère allusion lors de votre séjour à Berlin. Pour les formes binaires, on arrive par des transformations rationnelles toujours à des formes dont les déterminants sont en raison de *nombres carrés*, mais vous verrez bientôt que la chose est toute différente pour les formes ternaires et pour toutes celles d'un nombre impair d'indéterminées. Soit proposée, par exemple, la forme

$$x^2 + y^2 + z^2;$$

D étant un entier quelconque, elle se change par une substitution S de déterminant D^2, en général, dans une forme de déterminant D^4; mais si l'on ajoute la condition que tous les coefficients de la forme transformée soient divisibles par D, on obtient DF, la forme F ayant le nombre D pour déterminant. Cette forme est alors exprimée ainsi :

$$F = \frac{1}{D}[(\alpha x + \beta y + \gamma z)^2 + (\alpha' x + \beta' y + \gamma' z)^2 + (\alpha'' x + \beta'' y + \gamma'' z)^2],$$

le système linéaire

$$S = \begin{vmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{vmatrix},$$

étant assujetti à la condition que tous les coefficients de F soient des entiers.

La question principale est maintenant celle-ci : Quelles sont ces formes F de déterminant D qui naissent de la forme très-simple

$$\begin{pmatrix} \frac{1}{D}, & \frac{1}{D}, & \frac{1}{D} \\ 0, & 0, & 0 \end{pmatrix},$$

et pour chacune quelles sont les substitutions différentes?

Je trouve qu'en général toutes ces formes F appartiennent à des genres déterminés, et que, réciproquement, toutes les formes de ces genres ont la propriété dont il s'agit; pour le nombre des transformations il y a des théorèmes très-simples. Pour abréger, je suppose $D = pp'p''\ldots$ égal au produit de plusieurs nombres premiers inégaux, deux excepté. On a, dans ce cas, les théorèmes qui suivent. Nommons deux systèmes S et T équivalents à droite si l'on a une relation de la forme $S = T \times E$, et équivalents à gauche si ces systèmes sont liés par une relation de la forme $S = E \times T$, le signe $\times$ dénotant la composition des systèmes, et E étant un système quelconque de déterminant 1. Il faut bien distinguer ces deux notions d'équivalence pour les systèmes linéaires, c'est-à-dire pour les substitutions ou transformations; au reste, il existe quelque chose d'analogue pour les formes simultanées de degrés supérieurs. Cela posé, j'espère que vous donnerez votre approbation aux théorèmes suivants :

1. Toute forme

$$F = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

de déterminant $D = pp'p''\ldots$ et à coefficients entiers qui se tire de la forme

$$G = \begin{pmatrix} \frac{1}{D}, & \frac{1}{D}, & \frac{1}{D} \\ 0, & 0, & 0 \end{pmatrix}$$

par une transformation de déterminant D^2, a la propriété que l'un des trois nombres $b^2 - a'a''$, $b'^2 - aa'$, $b''^2 - aa'$ est résidu quadratique de D; plus généralement $\Phi \mathrm{R} D$ [*], Φ étant la forme adjointe de F, savoir,

$$\Phi = \begin{pmatrix} b^2 - a'a'', & b'^2 - aa'', & b''^2 - aa' \\ ab - bb'', & a'b' - bb'', & a''b'' - bb' \end{pmatrix},$$

c'est-à-dire que cette forme réunit les caractères $\Phi \mathrm{R} p$, $\Phi \mathrm{R} p'$, $\Phi \mathrm{R} p''$,

[*] D'après la notation de M. Gauss, pour exprimer que la forme Φ est résidu quadratique du nombre D. Ch. H.

et que tout nombre représentable par Φ et premier à p est résidu quadratique de p, que tout nombre représentable par Φ et premier à p' est résidu quadratique de p', etc. Remarquez que Φ est une forme négative, et ainsi

$$-\Phi = \begin{pmatrix} a'a'' - b^2, \ldots \\ \ldots\ldots\ldots \end{pmatrix}$$

une forme positive.

2. Cette condition est nécessaire, mais elle est aussi *suffisante*, et dans le genre auquel conviennent les caractères $\Phi R p$, $\Phi R p'$, $\Phi R p''$, etc. (genre principal si vous voulez), toute forme est renfermée dans G; ainsi *toutes les formes non équivalentes de ce genre se dérivent de la même source*.

3. La forme F étant une quelconque de ce genre, le nombre N total des transformations de G en F est $= 24 \cdot 2^\mu$, μ étant le nombre des facteurs premiers $p, p', p'', \ldots$, de D. Il est très-remarquable que ce nombre $24 \cdot 2^\mu$ est parfaitement indépendant de la classe individuelle à laquelle la forme F appartient, et toujours la même pour toutes les classes du genre entier. Le nombre des *substitutions non équivalentes à droite* ne monte qu'à $\frac{24 \cdot 2^\mu}{\delta}$ [*], δ se rapportant à F, car toutes ces N transformations de G en F se divisent naturellement en un nombre de groupes dont chacun contient δ substitutions équivalentes à droite, et qui se dérivent les unes des autres par la composition avec les transformations de F en elle-même dont le nombre est δ. Pour arriver à ces résultats, je m'occupe d'abord du problème d'assigner toutes les classes de substitutions (ou, si vous voulez, toutes les substitutions réduites) de déterminant D^2 par lesquelles la forme adjointe Φ d'une forme définie positive de déterminant D, se change en une forme divisible par D^2 (le quotient de la division sera une forme quelconque de déterminant 1 et ainsi équivalente à

[*] La quantité δ désigne, dans les travaux de M. Eisenstein, le nombre des transformations par lesquelles une forme quadratique ternaire se change en elle-même.

CH. H.

$x^2 + y^2 + z^2$). Je trouve le nombre de ces classes de substitutions par lesquelles Φ devient divisible par D^2, sans la moindre difficulté égal à 2^μ, supposé que la condition ΦRD soit remplie, autrement le problème n'a point de solution. Or vous verrez que le nombre des substitutions non équivalentes à gauche de G en F est le même que celui de ces classes de substitutions, c'est-à-dire égal à 2^μ (pour voir cela, pensez à la transposition des systèmes); enfin, on déduit de là le nombre total $24 \cdot 2^\mu$ des transformations de G en F, 24 étant le nombre des transformations de G en elle-même qu'il faut composer avec les 2^μ substitutions déjà trouvées. Dans ces recherches, il faut toujours bien distinguer l'ordre de la composition des substitutions.

4. F, F′, F″,... étant le système complet des formes non équivalentes de déterminant D et du genre dont il s'agit, et δ, δ', δ'',... étant les nombres de transformations en elles-mêmes, bien connus pour ces différentes formes respectivement, on obtient d'après le n° 3 pour le nombre des substitutions non équivalentes à droite, de G en F, de G en F′, etc., respectivement $\frac{24 \cdot 2^\mu}{\delta}$, $\frac{24 \cdot 2^\mu}{\delta'}$, $\frac{24 \cdot 2^\mu}{\delta''}$,..., ces substitutions étant réparties en raison de la densité [*].

Il suit de là que le nombre total de toutes les substitutions non équivalentes à droite, par lesquelles G se change dans une *quelconque* des formes F, F′, F″,..., monte à

$$\frac{24 \cdot 2^\mu}{\delta} + \frac{24 \cdot 2^\mu}{\delta'} + \frac{24 \cdot 2}{\delta''} + \ldots = 24 \cdot 2^\mu \sum \frac{1}{\delta}.$$

C'est donc aussi le nombre total des substitutions non équivalentes à droite par lesquelles la forme

$$x^2 + y^2 + z^2$$

se change en une forme divisible par D.

5. On peut, d'un autre côté, trouver ces substitutions par un procédé bien différent, en cherchant directement toutes les classes de

[*] Cette notion nouvelle et importante d'arithmétique transcendante se trouve exposée dans le Mémoire intitulé : *Neue theoreme der hoherer arithmetik*. Ch. H.

substitutions

$$\begin{vmatrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{vmatrix}$$

(toutes les substitutions réduites de déterminant D^2), qui satisfont à la congruence

$$(\alpha x + \beta y + \gamma z)^2 + (\alpha' x + \beta' y + \gamma' z)^2$$
$$+ (\alpha'' x + \beta'' y + \gamma'' z)^2 \equiv 0 \pmod{D},$$

qu'il faut résoudre indépendamment de x, y, z; je trouve le nombre des substitutions essentiellement différentes, c'est-à-dire des systèmes α, β, γ,..., non équivalents à droite (ou réduits) égal à

$$(p+1)(p'+1)(p''+1)\ldots.$$

6. Des n^os **5** et **4** comparés, on tire ce résultat remarquable,

$$24.2^\mu \sum \frac{1}{\delta} = (p+1)(p'+1)(p''+1)\ldots,$$

donc

$$\sum \frac{1}{\delta} = \frac{1}{24.2^\mu}(p+1)(p'+1)(p''+1)\ldots.$$

Voilà la démonstration d'un de mes théorèmes sur la quantité $\sum \frac{1}{\delta}$ [*], du moins pour le genre dont les caractères sont $\Phi R p$, $\Phi R p'$, $\Phi R p''$, etc.

7. Je fais une application de ce dernier résultat à la théorie des formes quaternaires, en démontrant que le nombre des représentations de D par la forme

$$x^2 + y^2 + z^2 + u^2$$

est égal à

$$8.24.2^\mu \sum \frac{1}{\delta} = 8(p+1)(p'+1)(p''+1)\ldots,$$

comme le trouve aussi M. Jacobi par la théorie des fonctions elliptiques.

---

[*] *Voir* le Mémoire cité plus haut. Journal de M. Crelle, tome XXXV. CH. H.