ANNALES SCIENTIFIQUES DE L'É.N.S.

KRONECKER

Sur une nouvelle propriété des formes quadratiques de déterminant négatif

Annales scientifiques de l'É.N.S. 1re série, tome 3 (1866), p. 287-294

<http://www.numdam.org/item?id=ASENS_1866_1_3__287_0>

SUR UNE NOUVELLE PROPRIÉTÉ

DES

FORMES QUADRATIQUES DE DÉTERMINANT NÉGATIF,

PAR M. KRONECKER.

(*Monatsbericht der Akademie der Wissenschaften zu Berlin*, 26 mai 1862.)

TRADUIT PAR M. HOÜEL,

PROFESSEUR A LA FACULTÉ DES SCIENCES DE BORDEAUX.

Les formules que j'ai trouvées, il y a cinq ans, pour le nombre des classes différentes des formes quadratiques de déterminant négatif, et qui ont été en partie communiquées à l'Académie en octobre 1857, m'avaient déjà conduit, vers cette époque, à étudier la cause intime des relations que j'y ai signalées entre certains déterminants, c'est-à-dire à chercher une dépendance entre les diverses formes quadratiques. Une induction, tirée de l'origine analytique de ces formules, m'amena très-promptement à la découverte de la dépendance soupçonnée; mais ce n'est que récemment que je suis parvenu à démontrer complétement, et par une méthode purement arithmétique, le résultat obtenu, qui fournit une relation entre les formes réduites de déterminants différents, et qui constitue l'objet de la présente communication.

p étant un nombre premier impair, imaginons que l'on ait formé toutes les formes quadratiques réduites positives des déterminants

$$-p, \quad -(p-1^2), \quad -(p-2^2), \quad -(p-3^2), \ldots,$$

dans lesquelles un au moins des coefficients extrêmes soit impair. Parmi les formes ambiguës qui se présentent, rejetons celles dans lesquelles $a = -2b$, ainsi que celles dans lesquelles $a = c$ et où b est en même temps positif. Enfin, pour toutes les formes restantes

$$(a_1, b_1, c_1), \quad (a_2, b_2, c_2), \quad (a_3, b_3, c_3), \ldots,$$

posons les congruences

$$a_1 z^2 + 2b_1 z + c_1 \equiv 0, \quad a_2 z^2 + 2b_2 z + c_2 \equiv 0, \ldots, \quad \text{mod. } p,$$

lesquelles auront évidemment ou une ou deux racines, suivant que le déterminant de la forme correspondante sera le nombre $-p$ lui-même, ou l'un des nombres $-(p-1)$, $-(p-4)$, $-(p-9)$,.... Si l'on désigne alors par $F(n)$ le nombre des classes différentes de déterminant $-n$, le nombre des racines de toutes ces congruences sera

$$F(p) + 2F(p-1^2) + 2F(p-2^2) + 2F(p-3^2) + \ldots,$$

et, par suite, en vertu de la formule (V) de ma Note insérée dans le *Journal de Crelle*, t. LVII, p. 249 (*), ce nombre sera égal à $p+1$ ou à p, suivant que l'on aura

$$p \equiv 1 \quad \text{ou} \quad p \equiv 3, \quad \text{mod. } 4.$$

Si maintenant, dans le premier de ces deux cas, pour les formes ambiguës dans lesquelles $a = c < \sqrt{p}$, on remplace par sa valeur négative une des deux racines de la congruence (savoir, celle qui correspond à la valeur positive de $\sqrt{b^2 - ac}$ *inférieure* à $\frac{1}{2}p$); et si, dans le cas unique où cette valeur est identique avec l'autre racine de la congruence, c'est-à-dire lorsque $b = 0$, on la laisse de côté, le nombre de toutes les valeurs formées de cette manière avec ces racines des congruences sera, dans tous les cas, égal à p. *Tous ces nombres sont différents suivant le module p, c'est-à-dire qu'ils forment, pour ce même module, la série complète des restes.*

De cette propriété remarquable des formes quadratiques de déterminant négatif, résulte immédiatement le théorème suivant :

Si l'on désigne par D, D′, D″,... *les différents nombres pour lesquels p est susceptible d'être représenté par les formes*

$$x^2 + \mathrm{D}y^2, \quad x^2 + \mathrm{D}'y^2, \quad x^2 + \mathrm{D}''y^2, \ldots,$$

y étant impair; si, de plus,

$$(a_1, b_1, c_1), \quad (a_2, b_2, c_2), \ldots$$

sont toutes les formes réduites positives proprement primitives de déterminants $-\mathrm{D}$, $-\mathrm{D}'$, $-\mathrm{D}''$,..., *les congruences*

$$a_1 z^2 + 2b_1 z + c_1 \equiv 0, \quad a_2 z^2 + 2b_2 z + c_2 \equiv 0, \ldots, \quad \text{mod. } p,$$

donnent, pour z, p valeurs toutes différentes entre elles, et dont chacune se présente

(*) *Voyez* la traduction de ce Mémoire, *Journal de Mathématiques de M. Liouville*, 2e série, t. V, 1860.

deux fois, pourvu que l'on fasse figurer deux fois les racines de toutes les congruences dans lesquelles le coefficient de z^2 n'a pas la même valeur absolue que l'un des deux autres coefficients.

Dans le cas de $p = 4n + 3$, comme il n'existe, pour aucun des déterminants $-D$, une forme ambiguë où l'on ait $a = \pm 2b$ ou $a = c$, le théorème précédent pourra s'énoncer plus simplement de la manière suivante :

Si (a_1, b_1, c_1), (a_2, b_2, c_2),... sont toutes les formes positives réduites proprement primitives de tous les déterminants négatifs $-D$ pour lesquels p peut être représenté par la forme principale $x^2 + Dy^2$, y étant impair, les racines des congruences

$$a_1 z^2 + 2b_1 z + c_1 \equiv 0, \quad a_2 z^2 + 2b_2 z + c_2 \equiv 0, \ldots, \quad \text{mod. } p,$$

formeront la série complète des restes pour le module p.

Enfin, si l'on considère les racines elles-mêmes de ces congruences du second degré, le théorème peut être formulé comme il suit, pour un nombre premier quelconque p :

Soit d un nombre entier et positif quelconque inférieur à $\sqrt{p}$, et soient, de plus, (a_1, b_1, c_1), (a_2, b_2, c_2),... toutes les formes réduites positives de déterminant $-(p - d^2)$, dans lesquelles un des deux coefficients extrêmes est impair, le coefficient moyen n'étant pas négatif. Les expressions

$$\frac{\pm b \mp d}{a}$$

formeront la série complète des restes pour le module p, si l'on admet, en général, les quatre combinaisons de signes, sauf deux exceptions, pour le cas de $a = 2b$, où l'on ne prendra b qu'avec le signe $-$, et pour le cas de $a = c$, où l'on ne prendra les deux nombres b et d qu'avec leurs signes supérieurs.

La démonstration de ce théorème se fonde, d'une part, sur la formule que j'ai citée tout à l'heure (*Journal de Liouville*, 2e série, t. V, p. 291), et à l'aide de laquelle on établit que le nombre des expressions telles que $\frac{\pm b \pm d}{a}$ est précisément égal à p; et, d'autre part, on fait voir que deux quelconques de ces expressions sont différentes entre elles suivant le module p. Des deux parties dont se compose, d'après cela, la démonstration, la première contient une déduction purement arithmétique de la formule en question pour les nombres de classes, tandis que la seconde partie établit comme il suit l'impossibilité de la congruence

$$a'(\pm b \pm d) + a(\mp b' \mp d') \equiv 0, \quad \text{mod. } p.$$

On fait voir d'abord que, dans l'équation

$$a'(\pm b \pm d) + a(\mp b' \mp d') = h.p,$$

qui tient lieu de la congruence, en ayant égard aux conditions d'inégalité auxquelles sont assujettis les nombres a, b, d, a', b', d', la valeur absolue de h ne peut être que zéro ou l'unité. Si maintenant cette équation a lieu, comme on peut disposer des signes dans le premier membre, de telle sorte que h soit positif, il n'y a plus à examiner que les deux cas de $h=0$ et de $h=1$, c'est-à-dire qu'il suffit d'établir l'impossibilité des deux équations

$$a'(\pm b \pm d) + a(\mp b' \mp d') = 0,$$
$$a'(\pm b \pm d) + a(\mp b' \mp d') = p.$$

Or, admettons, pour un instant, que les équations soient satisfaites par certaines valeurs de a, b, d, a', b', d', et que des deux quantités multipliées respectivement par a' et par a, la première soit positive. En désignant cette quantité par s, la première équation donnera les relations

$$a = a', \quad \pm b \pm d = \pm b' \pm d', \quad c \equiv c', \quad \text{mod. } s.$$

On reconnaît d'abord que $\frac{c-c'}{s}$ ne pourrait avoir que l'une des valeurs 0, ± 1, ± 2, et que, dans le premier cas, a, b, c seraient respectivement égaux à a', b', c', tandis que, dans le second cas, il faudrait, contrairement à la condition imposée, ou que a et c, ou que a' et c' fussent pairs à la fois. Dans le troisième cas, on aurait

$$\pm 2b = \mp 2b' = \pm a = \pm a',$$

ce qui serait en contradiction avec la convention établie relativement au choix des signes de b et de b'. Après avoir ainsi prouvé l'impossibilité de l'équation

$$a'(\pm b \pm d) + a(\mp b' \mp d') = 0,$$

on tirera de l'autre équation

$$a'(\pm b \pm d) + a(\mp b' \mp d') = p,$$

les expressions suivantes de a', b', c',

$$a' = na - 2b + s,$$
$$2b' = (mn-1)a - 2mb + c + (m-n)s,$$
$$c' = mc - (mn-1)s,$$

où l'on a écrit, pour abréger, b au lieu de $\pm b$, b' au lieu de $\mp b'$, m et n étant des entiers positifs, nuls ou négatifs. De ces trois équations on déduit enfin six relations, qui n'ont pas été obtenues sans difficulté, et qui constituent le point fondamental de la démonstration, en ce que, dans toutes les hypothèses que l'on peut

faire sur les nombres m et n, il est facile de démontrer l'incompatibilité de ces relations avec les conditions auxquelles sont soumis les nombres a, b, c, a', b', c'. Ces six équations sont les suivantes :

$$(c'-a')-m(a'+2b')+(m^2+m)a'+(a-2b)=(m-n+1)a,$$
$$(a'-2b')+(m-1)a'+(c-a)=ns,$$
$$m(a'-2b')+(c'-a')+(a-2b)+(m^2-m)(a-2b)+(m^2-m)s$$
$$=[m-(n-1)(m^2-m+1)]a,$$
$$(a'-2b')+(c-2b-1)+(m-2)(a-2b+s)+1=(n-1)(s+a-ma),$$
$$(a'-2b')+ma'+(c+2b-1)+1=(n+1)(a+s),$$
$$(c'-a')+(c-2b-1)+n(a+ms)+1=(m+1)c.$$

Dans les premiers membres de ces équations, on a renfermé entre parenthèses les combinaisons des nombres a, b, c, a', b', c', s, qui, en vertu des conditions d'inégalité, représentent des valeurs *non négatives*.

Le théorème arithmétique que l'on vient de démontrer est susceptible, comme il est facile de le voir, d'une généralisation, en ce sens que, au lieu du nombre premier p, on peut prendre un nombre composé. On peut, en outre, tirer de là des indications conduisant à une nouvelle déduction arithmologique des formules en question pour les nombres de classes, et ces indications paraissent d'autant plus importantes que la déduction arithmétique des formules en question, qui forme la première partie de la démonstration précédente, repose sur des considérations toutes différentes. J'ai porté, en effet, mon attention sur la manière dont Jacobi a démontré, dans le tome XII du *Journal de Crelle*, l'expression qu'il avait obtenue au moyen des séries (*Fundamenta nova, etc.*, p. 188), pour le nombre des décompositions en quatre carrés, et cela en transformant en quelque sorte les développements analytiques en développements arithmétiques. Par analogie avec cette méthode, j'ai représenté les nombres de classes des formes quadratiques de déterminant négatif sous forme de coefficients d'un développement, et j'ai donné quelques indications de ce procédé dans le tome LVII du *Journal de Crelle*. Mais je n'ai pas jugé à propos de publier la suite de mes résultats, parce qu'alors j'étais bien parvenu à un nouveau mode de vérification analytique des formules en question, mais je n'avais pas encore atteint le but principal, qui était d'en donner une démonstration arithmétique. Dans l'intervalle, M. Hermite a publié, dans une Note intéressante (*Comptes rendus, etc.*, 5 août 1861), quelques relations analogues, que je vais compléter ici, en exposant celles auxquelles j'ai été conduit, comme je viens de le dire, par la recherche d'une méthode de démonstration arithmétique.

Je conserverai, pour cela, toutes les notations et définitions dont j'ai fait usage dans le Mémoire plusieurs fois cité (*Journal de Crelle*, t. LVII, p. 248 et suiv., et

Journal de Liouville, 2e série, t. V, p. 289 et suiv.), et je renverrai, dans ce qui va suivre, aux formules I à VIII de ce Mémoire. Mais je supposerai que ces mêmes formules ont été transformées, de la manière développée p. 252 (p. 296 de la traduction), par l'emploi des fonctions F et G.

Si, dans les formules I, II, V, on multiplie les deux membres respectivement par q^{4n}, q^{2m}, $\frac{1}{2}q^{m}$; si l'on ajoute ensuite les trois équations ainsi obtenues, et que l'on fasse la sommation pour toutes les valeurs de n et de m, on obtiendra, à l'aide des expressions de X, Φ, Ψ, données p. 252 et suiv. (p. 296 de la traduction), l'équation

$$\sum \mathrm{F}(n)\,q^{n} = \frac{1}{2}\sqrt{\frac{\pi}{2\mathrm{K}}}\cdot\sum \frac{n}{q^{n}-q^{-n}}\left(q^{n^2+n}-2+q^{n^2-n}\right). \tag{1}$$

Les formules I, III, VI donnent pareillement

$$\sum \mathrm{F}(n)\,q^{n} = \frac{1}{2}\sqrt{\frac{\pi}{2k'\mathrm{K}}}\cdot\sum n(-q)^{n^2}\cdot\frac{q^{n}-q^{-n}}{q^{n}+q^{-n}}, \tag{2}$$

les lettres q, K, k', ainsi que les lettres k, Θ, H, que nous emploierons plus loin, étant prises avec les mêmes significations que dans les *Fundamenta* de Jacobi. Les deux équations ci-dessus expriment d'ailleurs précisément les relations contenues dans les formules I, II, III, V, VI, en développant suivant les puissances de q les sommes contenues dans les seconds membres. La formule IV peut se déduire comme conséquence des équations (1) et (2), après avoir tiré préalablement de celles-ci les relations :

$$\sum \mathrm{F}(2m)\,q^{\frac{1}{2}m} = \frac{k\mathrm{K}}{\pi}\cdot\sqrt{\frac{\mathrm{K}}{2\pi}},$$

$$\sum \mathrm{F}(4n+1)\,q^{n} = \frac{1}{q^{\frac{1}{4}}}\cdot\frac{\mathrm{K}}{\pi}\cdot\sqrt{\frac{k\mathrm{K}}{2\pi}},$$

$$\sum \mathrm{F}(8n+3)\,q^{2n} = \frac{1}{q^{\frac{3}{4}}}\cdot\frac{k\mathrm{K}}{2\pi}\cdot\sqrt{\frac{k\mathrm{K}}{2\pi}}.$$

Au moyen du développement de $\sin^2 \mathrm{am}\frac{2\mathrm{K}x}{\pi}$ suivant les cosinus des multiples de x (*Fundamenta*, p. 110), la série du second membre de l'équation (1) peut se mettre immédiatement sous la forme d'une intégrale définie, et, en introduisant les notations usitées,

$$\Theta\left(\frac{2\mathrm{K}x}{\pi}\right) = \vartheta_0(x), \qquad \mathrm{H}\left(\frac{2\mathrm{K}x}{\pi}\right) = \vartheta_1(x),$$

$$\vartheta_0\left(x+\frac{\pi}{2}\right) = \vartheta_2(x), \qquad \vartheta_1\left(x+\frac{\pi}{2}\right) = \vartheta_2(x),$$

on trouve ainsi

$$(3)\qquad \sum F(n)q^n = \frac{1}{q^{\frac{1}{4}}}\cdot\frac{k^2K}{2\pi^2}\cdot\sqrt{\frac{K}{2\pi}}\cdot\int_0^{\pi}\sin^2\operatorname{am}\frac{2Kx}{\pi}\cdot\vartheta_2(x)\cos x\,dx.$$

Cette relation, qui est, par suite, identique avec l'équation (1), peut être considérée comme une définition de la fonction $F(n)$. La détermination directe de l'intégrale donne aussi la signification arithmologique de $F(n)$, et, entre autres manières, on peut effectuer cette détermination en remplaçant $\sin^2\operatorname{am}\frac{2Kx}{\pi}$ par le carré du développement en série de $\sin\operatorname{am}\frac{2Kx}{\pi}$. Cette méthode m'a conduit, après diverses réductions et simplifications, à la démonstration arithmétique, dont j'ai parlé, des formules I, II, V, contenues dans la relation (3). De l'équation (3) on peut déduire toutes les formules de I à VIII. En remplaçant, en effet, sous le signe d'intégration, $\vartheta_2(x)$ par $\frac{1}{\sqrt{k'}}\vartheta_1(x)\cot\operatorname{am}\frac{2Kx}{\pi}$, la formule (3) devient

$$\sum F(n)q^n = \frac{1}{q^{\frac{1}{4}}}\cdot\frac{k^2K}{2\pi^2}\cdot\sqrt{\frac{K}{2\pi k'}}\cdot\int_0^{\pi}\sin\operatorname{am}\frac{2Kx}{\pi}\cos\operatorname{am}\frac{2Kx}{\pi}\vartheta_1(x)\cos x\,dx,$$

et l'on en tire l'équation (2), en remplaçant, sous le signe d'intégration,

$$\sin\operatorname{am}\frac{2Kx}{\pi}\cos\operatorname{am}\frac{2Kx}{\pi}$$

par son développement en série. De même, en substituant, dans l'équation (3), au lieu de

$$\vartheta_2(x)\sin^2\operatorname{am}\frac{2Kx}{\pi},$$

l'expression identiquement équivalente

$$\frac{1}{k^2}\vartheta_1(x) - \frac{1}{k\sqrt{k}}\cdot\cos\operatorname{am}\frac{2Kx}{\pi}\cdot\Delta\operatorname{am}\frac{2Kx}{\pi}\cdot\vartheta_3(x),$$

on trouve

$$\sum F(n)q^n - \frac{k\mathrm{K}}{2\pi}\cdot\sqrt{\frac{k\mathrm{K}}{2\pi}} = -\frac{1}{q^{\frac{1}{4}}}\cdot\frac{K}{2\pi^2}\cdot\sqrt{\frac{k\mathrm{K}}{2\pi}}\int_0^{\pi}\cos\operatorname{am}\frac{2Kx}{\pi}\Delta\operatorname{am}\frac{2Kx}{\pi}\vartheta_3(x)\cos x\,dx,$$

et l'on en tire la formule XI (*Journal de Crelle*, t. LVII, p. 253), en introduisant, sous le signe d'intégration, le développement obtenu par la différentiation de la formule (19), p. 101 des *Fundamenta* de Jacobi. Ainsi se trouve confirmée la con-

jecture que j'avais émise à la fin de mon Mémoire *sur le nombre des classes différentes des formes quadratiques*, les huit formules se tirant toutes d'une seule formule par des transformations analytiques. Mais, au point de vue arithmétique et algébrique, ces formules (*voyez* p. 252 du Mémoire) restent indépendantes les unes des autres, et contiennent explicitement toutes les nombreuses relations analogues que m'a fournies la théorie de la multiplication complexe des fonctions elliptiques, y compris aussi toutes celles que M. Hermite a données dans la Note citée plus haut. Dans une autre occasion, je développerai ce point, ainsi que les autres indications contenues dans la présente Note.