NOUVELLES ANNALES DE MATHÉMATIQUES

H. MINKOWSKI

Sur les propriétés des nombres entiers qui sont dérivées de l'intuition de l'espace

Nouvelles annales de mathématiques 3e série, tome 15 (1896), p. 393-403

<http://www.numdam.org/item?id=NAM_1896_3_15__393_0>

[I11b]

SUR LES PROPRIÉTÉS DES NOMBRES ENTIERS QUI SONT DÉRIVÉES DE L'INTUITION DE L'ESPACE;

PAR M. H. MINKOWSKI.

(Traduit de l'allemand, avec l'autorisation de l'auteur, par M. L. LAUGEL.)

Extrait des *Mathematical Papers read at the international Mathematical Congress held in connection with the world's Columbian Exposition Chicago* 1893 (New-York, Macmillan and C°, 1896).

Dans la théorie des nombres, comme dans chacun des autres domaines de l'Analyse, la découverte a lieu fréquemment au moyen de considérations géométriques, tandis qu'ensuite les vérifications analytiques sont peut-être seules communiquées. Par cela même, je ne serais pas en état d'épuiser mon thème, et ce n'est du reste pas mon dessein. Je me propose ici seulement de parler de cette configuration géométrique qui a avec les nombres entiers la relation la plus simple, je veux dire le *réseau des nombres*. Par ceci, un système quelconque de coordonnées cartésiennes x, y, z étant choisi dans l'espace, on doit entendre l'ensemble de tous les points x, y, z pour lesquels x, aussi bien que y et que z sont des nombres entiers. Pour faciliter l'intuition, on supposera que x, y, z sont des coordonnées rectangulaires habituelles.

Ainsi on a l'habitude d'employer une figure qui se présente comme découpée dans le réseau des nombres dans la démonstration de la règle de la multiplication : $(ab)c = a(bc)$. Je citerai aussi, pour plus de détails, les importantes relations relatives à la fonction (¹) $E(x)$ que Dirichlet (*Crelle*, t. 47, *Sur un problème relatif à la division*) a obtenues par des méthodes géométriques.

Mais je veux cependant m'en tenir ici aux questions où la notion de l'infini joue un rôle, c'est-à-dire où le réseau complet, et non simplement des découpures de ce dernier, est pris en considération.

Ce qui suit est la reproduction, en leurs parties principales, de quelques résultats de mon livre, *Géométrie des nombres* (1896, Teubner); je remarque, à ce propos, que dans mon livre la restriction aux systèmes de *trois* nombres entiers n'a pas lieu.

I. La notion la plus importante en corrélation avec le réseau des nombres, c'est celle du *volume* d'un corps; cette notion fournit alors plus tard les principes pour la définition de l'intégrale triple. Prenons chaque point du réseau des nombres pour centre d'un cube à faces parallèles aux plans des coordonnées et d'arête égale à 1. Avec chaque cube, on doit toujours aussi compter l'encadrement qui le délimite. On obtient ainsi une configuration N de cubes qui remplit l'espace sans lacunes, et chaque cube n'a aucun point intérieur en commun avec un autre. Soit maintenant un ensemble de points quelconque désigné par K, réparti tout entier sur un nombre fini de cubes de N. Dilatons cet ensemble K à partir d'un point quelconque p de l'espace dans toutes les directions et suivant un rapport quelconque $\Omega : 1$. Ainsi de K l'on déduira K_Ω^p. Soit alors a_Ω^p le nombre de *tous ceux des* cubes de N où chaque point est un point *intérieur* de K_Ω^p, et soit u_Ω^p le nombre de tous les cubes de N

(¹) Traduit par Houël dans le *Journal de Liouville*, t. I, p. 371.

qui contiennent toujours *au moins un* point de K_Ω^p. Cela posé, ainsi que l'a démontré M. Jordan (*Journ. de Math.*, 4e sér., t. VIII, p. 77; 1892), pour Ω croissant indéfiniment, $\Omega^{-3} a_\Omega^p$ et $\Omega^{-3} u_\Omega^p$ convergent toujours chacun vers des limites respectives déterminées A et U, indépendamment de p ; A et U sont dits les volumes *intérieur* et *extérieur* de K. On parlera simplement du volume de K lorsqu'on a $A = U$.

II. Maintenant les propriétés plus profondes du réseau des nombres dépendent d'une généralisation de la définition de la longueur d'une ligne droite, généralisation où l'on conserve seulement cette condition que dans un triangle la somme de deux côtés n'est jamais inférieure au troisième côté.

Concevons une fonction $S(ab)$ de deux points variables a et b quelconques, ne jouissant d'abord que des propriétés suivantes :

1° $S(ab)$ doit toujours être positif lorsque b est différent de a, et nul lorsque b et a sont identiques ; 2° si a, b, c, d désignent quatre points parmi lesquels b est différent de a et entre lesquels a lieu la relation $d - c = t(b - a)$, t étant *positif*, on doit alors toujours avoir $S(cd) = tS(ab)$. Cette relation doit être interprétée dans le sens du calcul barycentrique et signifie que les droites cd et ab ont même direction et que leurs longueurs (au sens ordinaire du mot) sont dans le rapport de $t : 1$. Pour distinguer du mot *longueur* dans son acception usuelle, on peut donner à $S(ab)$ le nom de *distance radiale de a à b* (Strahldistanz).

Soit o l'origine ; évidemment toutes les valeurs $S(ab)$ sont bien déterminées, pourvu que l'ensemble des points u soit donné pour lesquels $S(ou) \leqq 1$. Cet ensemble de points sera dit le *corps étalon* (Aich körper) des distances radiales. A ce corps en toute direction, à partir de o doit appartenir une droite issue de o de longueur finie, non évanouissante.

Maintenant ensuite, lorsque pour trois points quelconques a, b, c, on a toujours

$$S(ac) \leqq S(ab) + S(bc), \tag{3}$$

les distances radiales seront dites *concordantes* (einhellig). En ce cas, leur corps étalon jouit de cette propriété que, pour deux points quelconques u. v en ce corps, le segment de droite uv tout entier appartient à ce corps ; et, d'autre part, tout corps dont l'encadrement n'est *nulle part concave* et à l'intérieur duquel se trouve l'origine est corps étalon pour certaines distances radiales concordantes.

Par $E(ab)$ l'on désignera la moitié de l'arête du cube aux faces parallèles aux plans des coordonnées qui a pour centre a et dont l'encadrement passe par b. Les $E(ab)$ peuvent être regardées comme les $S(ab)$ concordantes les plus simples. J'ai exposé analytiquement la résolution complète des conditions fonctionnelles (1), (2), (3) dans le premier Chapitre de mon livre, *Géométrie des nombres*. La condition (3) a, en particulier, cette conséquence que la fonction $S(ab)$ est toujours une fonction *continue* des coordonnées de a et b, et ensuite qu'il se présente deux grandeurs positives g et G telles que l'on ait

$$g E(ab) \leqq S(ab) \leqq G E(ab)$$

pour tous les a et b, et enfin que le corps étalon possède un volume déterminé I. La signification de g et G est évidemment la suivante : le cube $E(ou) \leqq \frac{1}{G}$ est tout entier renfermé dans le corps étalon et ce dernier, de son côté, l'est tout entier dans le cube $E(ou) \leqq \frac{1}{g}$.

Les distances radiales $S(ab)$ seront dites *réversibles* wechselseitig) lorsqu'on a toujours

$$(4) \qquad S(ba) = S(ab).$$

Ceci a lieu au seul et unique cas où le corps étalon a l'origine pour *centre*.

III. Il existe évidemment, dans le réseau des nombres, des points r pour lesquels $E(or) = 1$.

Dans l'hypothèse de distances radiales *concordantes* quelconques $S(ab)$ l'on aura alors pour ces points r du réseau $S(or) \leqq G$. Maintenant cette dernière condition ne peut, en général, être remplie que par des points r tels que l'on ait $S(or) \leqq \frac{G}{g}$, et cette condition de plus n'est certainement remplie que par un nombre fini de points du réseau.

On reconnaît maintenant que, parmi toutes les distances radiales qui vont de o à tous les autres points du réseau, il en existe nécessairement une à valeur déterminée minima M et qui sera toujours $\leqq G$.

Si l'on construit alors, pour un premier point quelconque a du réseau, le corps $S(au) \leqq \frac{1}{2}M$, et pour un autre point quelconque c de ce réseau le corps $S(uc) \leqq \frac{1}{2}M$, ces deux corps, par suite de (3), n'ont aucun point intérieur en commun. Si l'on suppose, de plus, que les distances radiales sont aussi *réversibles*, le second corps est identique à $S(cu) \leqq \frac{1}{2}M$, et, par conséquent, alors les différents corps $S(au) \leqq \frac{1}{2}M$ relatifs aux différents points a du réseau des nombres s ont en commun au plus des points de leurs encadrements.

Soit maintenant Ω un nombre entier quelconque positif et pair, et construisons les corps en question pour tous les $(\Omega + 1)^3$ points.

$$x, y, z = 0 \pm 1 \pm 2 \pm \ldots \pm \frac{\Omega}{2},$$

renfermés dans le cube $E(au) \leqq \frac{\Omega}{2}$.

De $S(au) \leqq \frac{1}{2} M \leqq \frac{1}{2} G$ l'on conclut $E(au) \leqq \frac{1}{2} \frac{G}{g}$ et par suite tous ces corps seront renfermés dans le cube $E(au) \leqq \frac{1}{2}\left(\Omega + \frac{G}{g}\right)$ dont le volume est $\left(\Omega + \frac{G}{g}\right)^3$.

Maintenant, comme tous ces corps se confondent tout au plus en des points de leurs encadrements et qu'ils sont chacun de volume $\left(\frac{M}{2}\right)^3 I$, on en conclut l'inégalité

$$\left(\Omega + \frac{G}{g}\right)^3 \geqq (\Omega + 1)^3 \left(\frac{M}{2}\right)^3 I.$$

Maintenant M et I représentent des grandeurs déterminées et Ω peut être pris aussi grand que l'on veut, d'où l'on conclut

$$1 \geqq \left(\frac{M}{2}\right)^3 I. \tag{5}$$

Il doit donc par conséquent exister au moins un point q du réseau, différent de 0, *pour lequel on ait*

$$S(oq) \leqq \frac{2}{\sqrt[3]{I}}.$$

Le théorème ainsi obtenu, sur les corps à centre dont les surfaces limites ne sont nulle part concaves, me semble être l'un des plus féconds de toute la théorie des nombres. Inspiré par l'étude des travaux de Dirichlet et ceux de M. Hermite, sur les formes quadratiques (*Crelle*, t. 40, p. 209 et 291), je l'avais trouvé d'abord pour l'ellipsoïde; mais un plus grand intérêt encore s'attache aux conséquences que fournit ce théorème relativement aux formes linéaires; j'en expliquerai quelques-unes dans les § IV et V qui suivent.

Dans l'expression (5), le signe égal ne se présente que lorsque les corps $S(au) \leqq \frac{1}{2} M$, relatifs aux différents points a du réseau, remplissent l'espace *sans lacunes*. En ce cas, avant tout, l'encadrement complet du corps étalon doit être formé par un nombre fini de plans, nombre qui ne surpasse pas $2(2^3 - 1)$; en effet, chaque paroi plane de $S(au) \leqq M$, doit renfermer au moins un point du réseau x, y, z, et pour de tels points du réseau situés sur deux parois non symétriques par rapport à o, les nombres x, y, z ne peuvent jamais donner des résidus égaux pour le module 2, de même que pour aucun de ces points l'on ne peut avoir non plus $x, y, z \equiv 0, 0, 0 \pmod{2}$. Par exemple le signe égal ne se présente jamais dans (5) pour un octaèdre.

IV. Soient ξ, η, ζ trois formes linéaires en x, y, z, à déterminant D différent de zéro; supposons-les ou bien toutes les trois réelles, ou bien ξ réelle, et η et ζ deux formes à coefficients imaginaires conjugués; enfin, soit p une grandeur quelconque réelle. Le corps K_p, défini par

$$\left(\frac{|\xi|^p + |\eta|^p + |\zeta|^p}{3}\right)^{\frac{1}{p}} \leqq 1, \tag{6}$$

représente alors, pourvu que $p \geqq 1$, un corps dont la surface n'est nulle part concave. Pour le volume I_p de ce corps, on trouve

$$I_p = \frac{2^3}{\lambda_p^3 |D|}, \qquad \lambda_p^3 = \frac{3^{-\frac{3}{p}} \Gamma\left(1 + \frac{3}{p}\right)}{\left[\Gamma\left(1 + \frac{1}{p}\right)\right]^3}$$

ou bien

$$\lambda_p^3 = \frac{2}{\pi} \frac{3^{-\frac{3}{p}}\Gamma\left(1+\frac{3}{p}\right)}{\Gamma\left(1+\frac{1}{p}\right)2^{-\frac{2}{p}}\Gamma\left(1+\frac{2}{p}\right)};$$

l'on reconnaît enfin que pour un corps K_p, lorsque p est fini, le signe égal ne se présente jamais dans (5). On obtient ainsi ce théorème.

Lorsque $p \geqq 1$, *il existe toujours des nombres entiers* x, y, x, *qui ne sont pas tous nuls et pour lesquels on a*

$$\left(\frac{|\xi|^p + |\eta|^p + |\zeta|^p}{3}\right)^{\frac{1}{p}} < \lambda_p |D|^{\frac{1}{3}}.$$

Pour x, y, z constants, le premier membre de l'expression (6) décroît d'une manière continue avec p pour toutes les valeurs $p \geqq 0$, si l'on n'a pas $|\xi| = |\eta| = |\zeta|$, cas où cette expression serait indépendante de p (il en est du reste encore de même pour les valeurs négatives de p, lorsque aucune des grandeurs $|\xi|$, $|\eta|$, $|\zeta|$ n'est nulle). Par conséquent, chaque corps K_p sera contenu dans tous les autres de ces corps d'indice p plus petit et par suite $\frac{1}{I_p}$ et λ_p croissent d'une manière continue avec p; pour $p = \infty$, λ_p^3 converge respectivement vers 1, $\frac{2}{\pi}$. Pour $p = \infty$ K_p se transforme en le parallélépipède $-1 \leqq \xi \leqq 1$, $-1 \leqq \eta \leqq 1$, $-1 \leqq \zeta \leqq 1$; ou en le cylindre oblique à base elliptique $-1 \leqq \xi \leqq 1$, $\eta^2 + \zeta^2 \leqq 1$; K_1 au contraire représente un octaèdre ou les deux nappes d'un cône. Enfin pour $p = 0$ la fonction au premier membre de (6) converge vers la moyenne géométrique $\sqrt[3]{|\xi\eta\zeta|}$, en sorte que l'on peut ajouter encore le théorème suivant :

Il existe toujours des nombres entiers, qui ne sont *pas tous nuls et pour lesquels on a* $|\xi\eta\zeta| < \lambda_1^3 |D|$ *et par conséquent* a fortiori $< |D|$.

Ces théorèmes et leurs analogues, pour n formes linéaires à n variables, sont particulièrement susceptibles d'application dans la théorie des nombres algébriques, à la démonstration des théorèmes de Dirichlet sur les unités complexes et du théorème que le nombre des classes d'idéaux est fini, ils ont permis pour la première fois d'établir cette importante proposition que le discriminant de tout corps de nombres algébriques est divisible par au moins un nombre premier.

V. Soient a et b deux grandeurs réelles quelconques et t une grandeur quelconque > 1. L'application des théorèmes du n° III au parallélépipède

$$-1 \leqq x - az \leqq 1, \qquad -1 \leqq y - bz \leqq 1, \qquad -1 \leqq \frac{z}{t} \leqq 1,$$

nous fait voir qu'il existe toujours des nombres x, y, z, pour lesquels

$$0 < z \leqq t^{\frac{2}{3}}, \qquad |x - az| < \frac{1}{t^{\frac{1}{3}}}, \qquad |y - bz| < \frac{1}{t^{\frac{1}{3}}}.$$

Ce résultat, mais seulement au cas de valeurs entières de t, avait été déjà trouvé par Kronecker (*Berichte d. Berlin. Akad.*, 1884, p. 1073), au moyen de ce principe trivial en apparence, et néanmoins extraordinairement fécond [*voir* Dirichlet, *Généralisation d'un théorème de la Théorie des fractions continues*, (*Œuvres*), t. I, p. 636] que, lorsqu'un certain nombre de systèmes de grandeurs se distribuent en un nombre plus petit de domaines, deux au moins de ces systèmes doivent forcément être compris en un seul et même domaine. C'est là un exemple du petit nombre de cas où ce principe, plus simple, permet de tirer des conclusions essentiellement pareilles à celles données par le théorème arithmétique du § III.

La considération de l'octaèdre

$$|x - az| + \left|\frac{z}{t}\right| \leqq 1, \qquad |y - bz| + \left|\frac{z}{t}\right| \leqq 1$$

(en supposant $t \geqq 3$) montre l'existence de nombres entiers x, y, z, pour lesquels les deux expressions des premiers membres ci-dessus sont $< \left(\frac{3}{t}\right)^{\frac{1}{3}}$, tandis qu'en même temps $z > 0$; on trouve alors encore pour de tels nombres

$$\left|\frac{x}{z} - a\right| < \frac{3}{3z_{\frac{2}{3}}}, \qquad \left|\frac{y}{z} - b\right| < \frac{2}{3z_{\frac{3}{2}}}.$$

Ces propositions nous indiquent une voie par laquelle les résultats de la théorie des fractions continues sont susceptibles d'être généralisées avec succès.

VI. Si l'on considère des $S(ab)$ quelconques concordantes et réversibles, on aperçoit que 2^3 est la plus petite limite supérieure pour $M^3 I$. Si l'on s'en tient à la considération de distances radiales $S(ab)$ dont les corps étalons sont transformés *d'un* seul corps donné quelconque par l'effet de toutes les transformations homographiques possibles, l'origine restant fixe, on trouvera toujours dans cette classe restreinte de fonctions $S(ab)$ des fonctions telles que l'on ait

$$M^3 I > 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \ldots.$$

La démonstration de ce théorème nécessite une étude arithmétique de la théorie du groupe continu de toutes les transformations linéaires.

Finalement on peut ajouter que l'inégalité $M^3 I \leqq 2^3$, relative aux corps dont les surfaces à centre ne sont nulle part concaves, est susceptible encore d'une généralisation essentielle des plus remarquables, mais que je ne considérerai pas ici.