G. Poitou

Approximations diophantiennes et groupe modulaire

Séminaire Dubreil. Algèbre et théorie des nombres, tome 7 (1953-1954), exp. nº 7, p. 1-6
<http://www.numdam.org/item?id=SD_1953-1954__7__A7_0>

-:-:-:-:-:-

Séminaire d'ALGEBRE

Année 1953-1954

-:-:-:-:-

APPROXIMATIONS DIOPHANTIENNES ET GROUPE MODULAIRE

-:-:-:-:-

Conférence faite par G. POITOU, le 22 février 1954

-:-:-:-:-

J'ai choisi d'exposer quelques démonstrations, pour la plupart classiques, de la théorie des approximations diophantiennes, qui s'appuient directement sur la considération des groupes modulaires, pour faire observer, dans certains cas, leur puissance, et dans d'autres, leur instabilité.

I - Le groupe modulaire des entiers rationnels, formé des substitutions $z \longrightarrow \frac{az+b}{cz+d}$ à coefficients entiers a, b, c, d tels que $ad-bc = 1$ peut être considéré avec avantage comme opérant, non sur les z réels, mais sur les $z = x+iy$ complexes de partie imaginaire $y > 0$ (demi-plan de Poincaré) ce qui donne les formules de transformation

$$x' = \frac{(ax+b)(cx+d) + ac\, y^2}{(cx+d)^2 + c^2\, y^2} \qquad y' = \frac{y}{(cx+d)^2 + c^2\, y^2} .$$

De manière analogue, on peut faire opérer d'après Picard le groupe modulaire $z \longrightarrow \frac{az+b}{cz+d}$ à coefficients a,b,c,d entiers d'un même corps imaginaire quadratique $R(\sqrt{-m})$, tels que $ad-bc = 1$, sur un demi espace décrit par une variable complexe x et une variable positive y par les formules:

$$x' = \frac{(ax+b)(\overline{cx+d}) + a\bar{c}\, y^2}{(cx+d)(\overline{cx+d}) + c\bar{c}\, y^2} \qquad y' = \frac{y}{(cx+d)(\overline{cx+d}) + c\bar{c}\, y^2}$$

Rappelons que les entiers de $R(\sqrt{-m})$ constituent un module sur les entiers rationnels, dont une base est $(1, \omega)$ avec $\omega = \frac{1}{2}(1+\sqrt{-m})$ si $m \equiv 3 \pmod 4$, et $(1,\theta)$ avec $\theta = \sqrt{-m}$ si $m \equiv 1$ ou $2 \pmod 4$; et que l'opposé D du discriminant du corps vaut alors respectivement m et $4m$.

Le groupe opère transitivement sur les nombres du corps $z = p/q$ (p,q, entiers du corps) lorsque l'identité de Bézout est valable, c'est-à-dire pour un corps dénué d'idéaux non principaux (en fait, pour $D = 3,4,7, 8, 11, 19,\ldots$) cas auquel nous nous limiterons. En effet, il suffit de montrer qu'il existe une transformation du groupe amenant p/q en $1/0$ (le produit de celle-ci et de l'inverse de celle amenant p'/q' en $1/0$ transformant p/q en p'/q'). Or, il suffit de prendre $p = d$, $c = -q$, a et b étant fournis comme solutions de $ap + bq = 1$. Par cette transformation, on amène sur le plan $y' = \frac{h}{2}$ la sphère

$(cx+d)(\overline{cx+d}) + c\bar{c}\, y^2 = \frac{2}{h}\, y$ ou $|x - p/q|^2 + (y - 1/hq\bar{q})^2 = (1/hq\bar{q})^2$. Cette sphère, que nous désignerons par $S_h\ (p/q)$ est tangente au plan $y=0$ au point $x=p/q$, et a pour rayon $1/hq\bar{q}$ (Prendre garde que p/q doit être écrit sous forme irréductible).

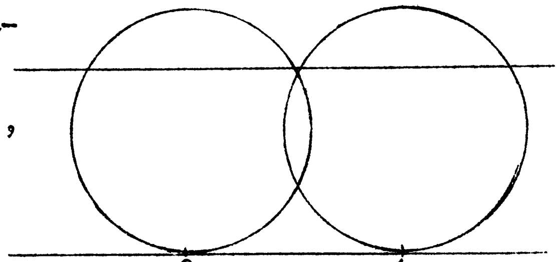
En considérant le plan $y = h/2$ comme la sphère "infinie" $S_h\ (1/0)$, l'ensemble des sphères $S_h\ (p/q)$ est invariant par le groupe, chaque sphère pouvant correspondre à n'importe quelle autre. En considérant $y \geqslant h/2$ comme l'intérieur (fermé) de $S_h\ (1/0)$ les intérieurs (fermés) se correspondent.

En convenant que "sphère" et "plan" peuvent signifier "cercle" et "droite", ceci s'applique au cas rationnel.

2 - De même qu'une forme quadratique définie positive $\alpha p^2 + 2\beta pq + \gamma q^2$ à variables p,q entières rationnelles est proportionnelle à $(p-qx)^2 + y^2q^2$, une forme hermitienne définie positive $\alpha p\bar{p} + \beta p\bar{q} + \bar{\beta}\bar{p}q + \gamma q\bar{q}$ à coefficients α et γ réels et β et $\bar{\beta}$ complexes conjugués, et dont les variables p,q sont des entiers d'un corps $R(\sqrt{-m})$ est proportionnelle à $(p-qx)(\overline{p-qx})+y^2q\bar{q}$, où x est complexe et y positif. Sous ces formes, le discriminant de l'une et de l'autre est $\Delta = y^2$.

Dire que le point (x,y) appartient à (l'intérieur fermé de) $S_h\ (p/q)$, c'est dire que $|p-qx|^2 + y^2|q|^2 \leqslant \frac{2}{h}\, y$. On en déduit que, si h est choisi de telle sorte que la réunion des $S_h\ (p/q)$ couvre tout le demi-espace $y > 0$, le minimum de toute forme est $\leqslant \frac{2}{h}\sqrt{\Delta}$. Pour qu'il en soit ainsi, il faut (c'est évident) et il suffit que la frontière de la sphère infinie soit recouverte par les autres sphères. En effet, le groupe étant transitif, il en sera de même pour chaque sphère ; le groupe étant discontinu pour $y > 0$, les sphères ne peuvent s'accumuler en un point de cette région ; si celle-ci n'était pas couverte par la réunion des sphères, il y aurait des points frontières de cette région sur la frontière d'une sphère, ce qui est impossible.

Dans le cas rationnel, cette condition s'exprime par $h \leqslant \sqrt{3}$. En effet, si $h \leqslant \sqrt{3}$, les cercles $S_h\ (p/1)$ recouvrent la droite $y = h/2$; si $h > 3$, ces cercles ne suffisent pas et les autres ne peuvent compenser, puisque leur rayon est au plus $1/4h < 1/4\sqrt{3}$ alors que $h/2 > \sqrt{3}/2 > 2/4\sqrt{3}$.



0 1

Fig.1

De ceci résulte que pour toute forme quadratique $F(p,q)$ définie positive, le minimum pour $(p,q \neq (0,0)$ est au plus $\frac{2}{\sqrt{3}}\sqrt{\Delta}$, la constante $\frac{2}{\sqrt{3}}$ étant "exacte", ce qui équivaut au fait que le "déterminant critique" du cercle de rayon 1 est $\sqrt{3}/2$.

Dans les cas complexes, soit r le plus petit rayon de cercles tous égaux centrés aux entiers du corps qui recouvrent le plan (r est le rayon du cercle circonscrit au triangle isocèle $0, 1, \omega$ ou au rectangle $0, 1, \theta, \theta+1$, donc vaut $k/\sqrt{m}$ ou $\frac{1}{2}\sqrt{1+m}$ suivant que $m \equiv 3$ ou non (mod 4), en posant dans le premier cas $m = 4k-1$). Pour que les sphères $S_h(p/1)$ recouvrent le plan $y = h/2$, il faut et il suffit que le rayon des cercles d'intersection, soit $\sqrt{1-\frac{h^2}{4}}$, soit au moins égal à r , ce qui donne les conditions suffisantes $h^2 \leq 4(1-\frac{k^2}{m})$ ou $3-m$. Ceci implique que le minimum pour $(p,q) \neq (0,0)$ d'une forme hermitienne $F(p,q)$ définie positive est au plus $\frac{2}{H}\sqrt{\Delta}$, les constantes H étant données par le tableau:

$D =$	3	4	7	8	11
$H =$	$2\sqrt{\frac{2}{3}}$	$\sqrt{2}$	$2\sqrt{\frac{3}{7}}$	1	$2\sqrt{\frac{2}{11}}$

La réciproque n'est pas assurée, dans les mêmes conditions que pour le cas rationnel, donc la constante H à coup sûr "exacte", que si $H/2 \geq 1/H$, donc pour $D = 3$ ou 4 [1] .

D'autre part, écrivant $F(p,q) = P\bar{P} + Q\bar{Q}$ avec $P = \lambda p + \mu q$, $Q = \rho p + \sigma q$, on déduit du fait que le déterminant critique de la sphère à 4 dimensions vaut $\frac{1}{2}$ [2] , que le minimum de F est au plus $\sqrt{\frac{D}{2}}\sqrt{\Delta}$; ce qui fournit - chose curieuse - exactement les mêmes valeurs que précédemment, sauf dans le cas $D = 7$, où le résultat est moins bon . Par contre, cette méthode donne un résultat général alors que la précédente se dérobe en dehors des cas écrits.

3 - Les figures évoquées peuvent aussi servir à étudier l'approximation des nombres réels par des rationnels, puis des nombres complexes par des nombres p/q d'un corps $R(\sqrt{-m})$. La remarque essentielle est que la relation $|x - \frac{p}{q}| \leq \frac{1}{hq\bar{q}}$ équivaut à l'affirmation que pour un certain $y > 0$, le point (x,y) appartient à $S_h(p/q)$ - ou encore, que la droite perpendiculaire au plan $y = 0$ au point x coupe la sphère $(S_h - p/q)$.

Posons $C(x) = \overline{\lim}\ 1/|q(qx-p)|$ (constante d'approximation de x) et $C = $ b. inf. $C(x)$ ("constante d'Hurwitz" du corps envisagé).

Si la droite perpendiculaire au plan $y=0$ au point x coupe une infinité de $S_h(p/q)$, c'est que $h \leqslant C(x)$; si ceci se produit pour tout x qui n'est pas dans le corps, c'est que $h \leqslant C$.

Nous utiliserons une condition <u>suffisante</u> que nous appellerons le "principe des trous" [1]. Appelons <u>trous</u> les composantes connexes du complémentaire (dans le demi-espace $y > 0$) de la réunion des sphères (fermées) $S_h(p/q)$; <u>borné</u> (suivant Poincaré) un ensemble du demi-espace qui est borné au sens ordinaire, et à distance strictement positive du plan $y = 0$.

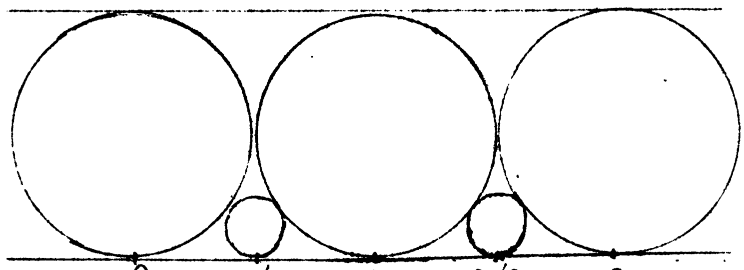


fig. 2

<u>Principe des trous</u> : Si, pour un certain h, les trous sont bornés, $C \geqslant h$. En effet, en se déplaçant sur la droite perpendiculaire au point x au plan $y = 0$, dans le sens des y décroissants, on finit par sortir de chaque trou; mais, x étant hors du corps, on sort aussi de chaque sphère; donc on rencontre une infinité de sphères. Conséquence immédiate: $C \geqslant H$ (défini au § 2). Mais il y a mieux; examinons d'abord le cas rationnel; on a non seulement $C \geqslant \sqrt{3}$, mais $C \geqslant 2$, comme le montre la figure 2 ; en effet, pour que tous les trous soient bornés, il suffit, puisque tous les trous sont équivalents par le groupe, que le soient ceux que borde le cercle infini ; et pour ceux-ci, il suffit de constater que les cercles $S_2(p/1)$ sont tangents entre eux et à $S_2(1/0)$.

En fait, on sait que $C = \sqrt{5}$ [3] ; ceci peut se démontrer sur une telle figure, mais exige quelques calculs [4] . Si l'on passe aux cas complexes, on est amené généralement à des calculs beaucoup plus compliqués [5] ; mais il se trouve qu'on peut obtenir très simplement des résultats puissants. Examinons d'abord ce qu'on peut déduire, par le principe des trous, de la considération des seules sphères $S_h(1/0)$ et $S_h(p/1)$. En donnant à r le même sens qu'au § 2, on exprime que ces sphères enferment des trous en écrivant d'abord que les sphères $S_h(p/1)$ recouvrent le plan de leurs centres, soit $1/h \geqslant r$. Si cette condition suffisait, on aurait démontré:

$D =$	3	4	7	8	11	19
$C \geqslant$	$\sqrt{3} = 1,73$	$\sqrt{2} = 1,41$	$\sqrt{7}/2 = 1,32$	$2/\sqrt{3} = 1,15$	$\sqrt{11}/3 = 1,10$	$\sqrt{19}/5 = 0,87$

alors que les valeurs exactes sont:

$$\sqrt[4]{13} = 1{,}89 \quad \sqrt{3} = 1{,}73 \quad \sqrt[4]{8} = 1{,}68 \quad \sqrt{2} = 1{,}41 \quad \sqrt{5}/2 = 1{,}11 \quad 1$$

[6] [7] [5] [8] [9] , [10] [10]

L'inégalité paraît donc numériquement excellente; mais l'application du principe des trous exige que le plan S_h (1/0) soit au-dessus du plan des centres des S_h (p/1), et la limitation n'est correcte que pour D = 3 et 4 .

Par compensation, pour le corps de Gauss (D = 4), le principe des trous donne le résultat "exact" $C = \sqrt{3}$, à condition de considérer aussi les sphères S_h (p/1+i) de rayon 1/2h.

Il suffit en effet, pour montrer que $C \geqslant \sqrt{3}$, de constater que les 6 sphères $S_{\sqrt{3}}(1/0)$, $S_{\sqrt{3}}(0/1)$, $S_{\sqrt{3}}(1/1)$, $S_{\sqrt{3}}(i/1)$, $S_{\sqrt{3}}(1+i/1)$ et $S_{\sqrt{3}}(1/1-i)$ délimitent un trou; pour cela, il suffit de vérifier que ces 6 sphères recouvrent les faces de l'octaèdre obtenu en joignant les centres des deux sphères extrêmes $S_{\sqrt{3}}(1/0)$ et $S_{\sqrt{3}}(1/1-i)$ aux quatre autres centres; ce qui est immédiat (fig.3; revoir la fig.1).

On a donc obtenu, d'une manière étonnamment simple ([1] ; voir aussi [7]) que l'inégalité $\left| x - \frac{p}{q} \right| \leqslant \frac{1}{\sqrt{3}\, q^2}$ a une infinité de solutions en entiers de Gauss p,q, pour tout x complexe hors du corps.

Le caractère "exact" de la constante $\sqrt{3}$ résulte d'un exemple facile (voir par exemple [10] , 11.6).

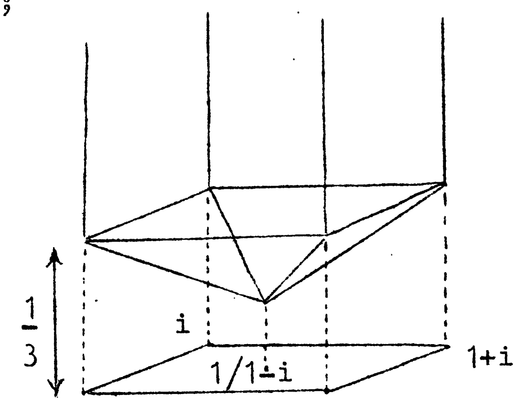


fig.3

4 - Les méthodes précédentes peuvent être appliquées à des problèmes d'un type un peu différent. Indiquons d'abord ce théorème:

s étant un entier $\geqslant 2$, il existe une infinité de fractions p/q telles que $\left| x - \frac{p}{q} \right| \leqslant \frac{1}{2q^2}$, q n'étant pas divisible par s ; la constante 2 est "exacte" si s = 2 (ce qui résulte encore d'un exemple); si $s \neq 2$, on peut remplacer cette constante 2 par $\sqrt{5}$; laquelle constante est évidemment "exacte", puisqu'elle l'est déjà sans la condition supplémentaire $q \not\equiv 0 \pmod s$.

Le cas s = 2 est bien connu [11] ; le reste est dans [12] .

En d'autres termes, en désignant par C(s) la constante analogue à C sous la condition supplémentaire $q \not\equiv 0 \pmod s$, on a $C(2) = 2$ et $C(s) = \sqrt{5}$ pour $s \neq 2$.

La démonstration de $C(2) \geqslant 2$ est immédiate sur la fig.2. Qualifions en effet, de mauvais ou de bon un cercle $S_2(p/q)$ selon que q est ou n'est pas divisible par s . Remarquons que les trous bordant le cercle infini sont limités par un mauvais et deux bons cercles ; il est aisé de prouver qu'il en va de même pour tous les trous ; d'où résulte que toute droite perpendiculaire à $y = 0$ en un point x irrationnel coupe une infinité de bons cercles, et par suite le théorème en question.

Passons aux cas complexes. Si $D = 3$, il n'y a encore qu'une mauvaise sphère parmi les 4 sphères $S_{\sqrt{3}}(1/0)$, $S_{\sqrt{3}}(0/1)$, $S_{\sqrt{3}}(1/1)$, $S_{\sqrt{3}}(\omega/1)$ qui enserrent un trou et ceci reste vrai pour chaque trou, donc $C(s) \geqslant \sqrt{3}$ pour tout s qui n'est pas une unité.*

Si $D = 4$, le même raisonnement est valable pour les six sphères considérées à la fin du § 3 , pourvu que $|s|^2 > 2$, donc dans ce cas $C(s) = \sqrt{3}$ car déjà $c = \sqrt{3}$. Une variante permet de traiter le cas $|s|^2 = 2$ (soit par exemple $s = 1+i$) , comme me l'a signalé R. Descombes. En effet, comme on l'a vu au § 2 , les sphères $S_{\sqrt{2}}(p/1)$ (qui sont bonnes) recouvrent la frontière de la sphère infinie ; donc toute mauvaise sphère a sa frontière recouverte par des bonnes sphères, et l'on peut rencontrer une mauvaise sphère sans par là même en rencontrer de bonnes, ce qui prouve qu'on rencontre encore une infinité de bonnes sphères, et que $C(1+i) \geqslant \sqrt{2}$.*

Références

[1] Speider, Über die Minima Hermitescher Formen, J. Crelle 167, p.88 (1932)

[2] Korkine et Zolotareff, Sur les formes quadr. Math. Ann. 5, p.581, (1872)

[3] Hurwitz, Über die angenäherte Darstellung ... Math. Ann. 39, p.279, (1889)

[4] Humbert, trois articles dans le journal de Liouville de 1916.

[5] Hofreiter, Diophantische Approximationen ... Mh. Math. 45, p.175, (1936)

[6] Perron, Über einer Approximationssatz ... S.B. Bayer. (1931) p. 129.

[7] Ford, On the closeness of approach ... Trans. Am. Math. Soc. 27, p.146, (1925)

[8] Perron, Diophantische Approximationen ... Math. Z. 37, p.749, (1933)

[9] Descombes et Poitou, Sur l'approximation ... C.R. 231, p.264, (1950)

[10] Poitou, Sur l'approximation des nombres ... Ann. Ec. N. 70, p.199, (1953)

[11] voir à ce sujet les nombreuses références de [12].

[12] Descombes, Etude diophantienne de certaines formes ... Bull. Soc. Math. (à paraître).

* R. Descombes signale que des exemples appropriés lui permettent d'affirmer que, pour $D = 3$, $C(1+\omega) = \sqrt{3}$; et, pour $D = 4$, $C(1+i) = \sqrt{2}$. Les valeurs de $C(s)$ pour le corps de Gauss offrent donc une analogie avec celles du cas rationnel.