Séminaire Dubreil.
Algèbre et théorie
des nombres

G. Poitou

Sur les formes linéaires complexes

Séminaire Dubreil. Algèbre et théorie des nombres, tome 10 (1956-1957), exp. n° 6, p. 1-5
<http://www.numdam.org/item?id=SD_1956-1957__10__A6_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire P. DUBREIL et C. PISOT
(ALGÈBRE et THÉORIES DES NOMBRES)
Année 1956/57
-:-:-:-

Exposé n° 6

SUR LES FORMES LINÉAIRES COMPLEXES.

(Exposé de G. POITOU, le 17.12.1956)

Dans cette conférence, j'ai l'intention d'exposer comment on pourrait refaire le dernier chapitre du livre de MINKOWSKI "Diophantische Approximationen" paru en 1907.

Il s'agit du minimum simultané de deux formes linéaires complexes $\alpha x + \beta y$, $\gamma x + \delta y$, où les variables x , y sont des entiers, par exemple de Gauss, non tous deux nuls.

Dans le cas réel, soient α , β , γ , δ des nombres réels de déterminant $\alpha\delta - \beta\gamma \neq 0$. Il existe alors des entiers rationnels x , y non tous deux nuls tels que

$$|\alpha x + \beta y| \leq \sqrt{|\alpha\delta - \beta\gamma|} \quad , \quad |\gamma x + \delta y| \leq \sqrt{|\alpha\delta - \beta\gamma|}$$

Dans le cas complexe, soit $\mathcal{a}$ un réseau de nombres complexes (c'est-à-dire un module de nombres complexes, discret et de rang 2) et α , β , γ , δ des nombres complexes de déterminant non nul. Il existe alors des constantes μ telles que, sur des nombres x , y de $\mathcal{a}$ non tous deux nuls,

$$|\alpha x + \beta y|^2 \leq \mu |\alpha\delta - \beta\gamma| \quad , \quad |\gamma x + \delta y|^2 \leq \mu |\alpha\delta - \beta\gamma| \quad ,$$

et le lemme familier de MINKOWSKI sur les jauges permet d'affirmer que $\frac{4}{\pi}\Delta$ est une telle constante, où Δ est la valeur absolue du déterminant d'une base quelconque de $\mathcal{a}$ sur les entiers rationnels.

J'ai indiqué ailleurs qu'on peut prendre aussi $\sqrt{\frac{4}{\pi}\frac{2}{\sqrt{3}}}\Delta$ et peut être $\frac{2}{\sqrt{3}}\Delta$.

Quoi qu'il en soit, désignons par $M(\mathcal{a})$ la borne inférieure des nombres μ convenant pour le réseau $\mathcal{a}$.

Dans toute la suite, on supposera que $\mathcal{a}$ est un ordre quadratique imaginaire (c'est-à-dire un anneau d'entiers d'un corps quadratique imaginaire, contenant 1 et engendrant le corps par quotients).

Les résultats de MINKOWSKI peuvent s'énoncer ainsi pour l'essentiel: la valeur de cette constante est

$\frac{\sqrt{2}}{3-\sqrt{3}}$ pour $\mathcal{a}$ engendré par 1 et $\sqrt{-1}$

1 pour $\mathcal{a}$ engendré par 1 et $\frac{1}{2}(1+\sqrt{-3})$

Les méthodes habituelles ramènent la définition de $M(\mathcal{a})$ à la suivante :

Soit $\mathcal{B}$ la jauge de l'espace de deux variables complexes (z_1 , z_2) définie par les inégalités :

$$\times \; |z_1| < 1 \qquad\qquad |z_2| < 1$$

Appelons désormais <u>réseau</u> un $\mathcal{a}$-module discret de rang 2 ; disons qu'il <u>est admissible pour</u> $\mathcal{B}$ s'il n'a dans $\mathcal{B}$ que le point 0 . Alors $1/n(\mathcal{a})$ est la borne inférieure des masses des réseaux admissibles pour $\mathcal{B}$; la <u>masse</u> d'un réseau étant le module du déterminant d'une base quelconque (sur $\mathcal{a}$) de ce réseau.

On voit facilement, comme MINKOWSKI, que $1/M(A)$ est aussi la borne inférieure des masses des réseaux <u>réduits</u>, c'est-à-dire des réseaux admissibles qui contiennent des points

$A = (-u , 1)$ avec $|u| < 1$ et $B = (1 , -v)$ avec $|v| < 1$.

Mais si ces points s'expriment sous la forme

$$A = p'C + q'D \qquad\qquad B = pC + qD .$$

en fonction d'une base (C , D) du réseau considéré, celui-ci a pour masse

$$\left| \frac{1 - uv}{d} \right|$$

avec $d = pq' - qp'$

tandis que l'admissibilité du réseau considéré s'exprime par l'incompatibilité des deux systèmes suivants :

(1) $ap' + bp \equiv 0 \pmod d$ $\quad aq' + bq \equiv 0 \pmod d$ $\quad a , b \in \mathcal{a}$

(2) $|au - b| < |d|$ $\quad |a - bv| < |d|$ $\quad (a , b) \neq (0 , 0)$

Ainsi $M(\mathcal{a})$ est égal à la borne supérieure de $\left|\frac{d}{1-uv}\right|$, où u , v , d sont des nombres complexes vérifiant

(3) $|u| < 1$ $\quad |v| < 1$ $\quad d = pq' - qp'$ $\quad p , q , p' , q' \in \mathcal{a}$

tels que (1) et (2) soient incompatibles.

Pour aborder le problème plus simplement, on peut commencer par remplacer (2) par l'un ou l'autre des systèmes

$$(2') \qquad |a| + |b| < |d| \qquad (a , b) \neq (0 , 0)$$

$$(2'') \qquad |a| + |b| \leq |d| \qquad ab \neq 0$$

Supposons alors que l'ordre $\mathcal{O}$ soit principal, c'est-à-dire que l'absence d'idéaux non principaux permette d'y appliquer les règles ordinaires de l'arithmétique. Il en résulte que p et q (et de même p' et q') sont premiers entre eux ; car si l'on avait

$$p = mp_1 \qquad q = mq_1 \qquad m , p_1 , q_1 \in \mathcal{O} , \quad |m| > 1$$

on aurait $d = md_1$, $d_1 \in \mathcal{O}$ et on obtiendrait une solution commune à (1) et à (2') (donc à (2)) en prenant $a = 0$ $b = d_1$. On voit alors facilement par combinaison linéaire que (1) équivaut à

$$(1') \qquad b \equiv s\,a \pmod{d} \; ; \quad a , b \in \mathcal{O}$$

où s est un nombre de $\mathcal{O}$ premier avec d .

En prenant $a = 1$ $b \equiv s \pmod{d}$, ou $b = 1$ $a \equiv s^{-1} \pmod{d}$, on satisfait (1') et aussi (2'') si la classe de s , ou de s^{-1} , mod d , contient un nombre de modules au plus égal à $|d| - 1$. Il faut donc exclure les valeurs de l'entier d telles que les classes premières à d soient représentables, soit elles-mêmes, soit leurs inverses, par des nombres de module au plus égal à $|d| - 1$.

Ce résultat s'applique en particulier au cas réel, $\mathcal{O}$ étant l'anneau des entiers rationnels, et montre qu'alors on a nécessairement $d = \pm 1$. Ce résultat équivaut au fait que deux réduites consécutives du développement en fraction continue d'un nombre réel quelconque, définies a priori par leurs qualités d'approximation, ont un déterminant égal à ± 1 . La même méthode, avec une dimension de plus, permet de démontrer simplement le théorème de Furtwängler qui affirme que le déterminant de trois triplets réduits consécutifs, pour l'approximation simultanée de deux nombres réels, est en module 0 , 1 ou 2 .

Appliquons ceci, par exemple, à l'anneau de tous les entiers de Gauss $a + bi$ (a , b entiers rationnels). On voit alors, d'après la majoration

initiale de M, que

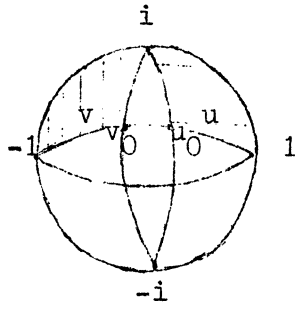
$$|d|^2 < 5{,}9$$

Donc, à une unité près et à la conjugaison près, $d = 1$, $1 + i$, 2 ou $2 + i$.

Si $d = 2 + i$, un système complet de restes mod. d est $(0, \pm 1, \pm i)$; les modules de ces nombres sont au plus 1, inférieurs à $\sqrt{5} - 1$, donc ce cas est exclu.

De même, si $d = 2$, les classes premières à d (mod d) sont représentées par 1 et i, de module $1 \leqslant 2 - 1$, donc ce cas est exclu.

Si $d = 1 + i$, (1') prend la forme $b \equiv a \mod (1 + i)$ et l'on voit



alors facilement que u et v sont, à des symétries près, astreints à se trouver dans les régions hachurées ci-contre, et que

$$\text{b.inf } |1 - uv| = |1 - u_0 v_0| = 3 - \sqrt{3} \quad \text{d'où}$$

$$\text{b. sup } \left|\frac{d}{1 - uv}\right| = \frac{\sqrt{2}}{3 - \sqrt{3}} \quad \text{dans ce cas}$$

le fait que le min. de $|1 - uv|$ est <u>atteint</u>, et en des points intersections de cercles limitant, conformément à (2), les régions permises pour u et v, remarqué sans démonstration par MINKOWSKI, se démontre sans difficulté et correspond au fait géométrique qu'un réseau "critique" a (sauf le cas où u ou $v = 0$) au moins trois points tels que A et trois points tels que B. En faisant jouer cette remarque, on voit que le minimum, dans le deuxième cas à examiner $d = 1$, de $|1 - uv|$ correspond à un réseau qui contient d'autres points A et B correspondant à un déterminant égal à $1 + i$; donc la borne supérieure de $\left|\frac{d}{1 - uv}\right|$ ne peut être strictement supérieure à la précédente ; et ceci démontre que la constante M, pour cet anneau des entiers de Gauss, est bien $\frac{\sqrt{2}}{3 - \sqrt{3}}$.

Supposons maintenant que l'ordre $\mathcal{O}$ ne soit plus principal ; on montre alors que la fraction p/q doit être <u>irréductible</u>, en ce sens qu'il n'existe pas de fraction égale à termes plus petits ; ce qui signifie aussi que l'idéal (p, q) est <u>minime</u>, en ce sens qu'il a une norme minimum, parmi les idéaux de la même classe. Il ne peut donc parcourir qu'un ensemble fini d'idéaux.

Par exemple, dans l'anneau de base $[\ 1\ ,\ \omega = \frac{1}{2}(1 + \sqrt{-15})\ ]$, il y a deux classes d'idéaux, et les idéaux minimes de la classe non principale sont $(2\ ,\ \omega)$ et $(2\ ,\ \bar{\omega})$, dont la norme est 2. Pour un tel anneau quatre cas sont possibles :

ou bien les idéaux $(p\ ,\ q)$ et $(p'\ ,\ q')$ sont égaux à 1
ou bien l'un d'eux est égal à 1, et l'autre à $(2\ ,\ \omega)$ ou $(2\ ,\ \bar{\omega})$
ou bien tous deux sont égaux à $(2\ ,\ \omega)$ par exemple
ou bien l'un est égal à $(2\ ,\ \omega)$, l'autre à $(2\ ,\ \bar{\omega})$

Dans les deux premiers cas, on réduit encore (1) à la forme (1'), sauf que dans le deuxième cas s n'est plus nécessairement premier avec d.

Dans les deux derniers cas, on peut supposer, par combinaison linéaire, qu'on a par exemple $p = 2$, $q = \omega$, et comme par ailleurs d doit être divisible par le produit des idéaux $(p\ ,\ q)$ et $(p'\ ,\ q')$, c'est-à-dire que $|d|$ doit être égal (compte tenu de la majoration générale de M donnée au début) à 2 ou à 4, des lemmes appropriés permettent d'affirmer que $|d| = 2$ et que (1) se réduit à

$d = 2$ $\qquad a \in (2\ ,\ \omega)$ $\qquad b \in (2\ ,\ \bar{\omega})$ ou inversement, ou bien
$d = \omega$ $\qquad a \in (2\ ,\ \omega)$ $\qquad b \in (2\ ,\ \bar{\omega})$ à la symétrie près.

Compte tenu des premières possibilités, on trouve qu'il est nécessaire d'étudier le minimum de $(1 - uv)$ dans huit cas différents ; mais ici encore, on peut simplifier ce travail.

Quoi qu'il en soit, on voit que la présence d'idéaux non principaux, si elle n'est pas un obstacle insurmontable, est tout de même assez gênante.