Séminaire Dubreil.
Algèbre et théorie
des nombres

Claude Chabauty

Sur les formes algébriques de type compact

Séminaire Dubreil. Algèbre et théorie des nombres, tome 9 (1955-1956), exp. n° 25, p. 1-5
<http://www.numdam.org/item?id=SD_1955-1956__9__A19_0>

Faculté des Sciences de Paris
-:-:-:-

28 mai 1956

Séminaire P. DUBREIL et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1955/56
-:-:-:-

Exposé N° 25

SUR LES FORMES ALGÉBRIQUES DE TYPE COMPACT

par Claude CHABAUTY

-:-:-:-

1.- Enoncé des résultats

(A) Une forme quadratique, à coefficients réels, indéfinie est arithmétiquement équivalente à une forme dont les coefficients sont bornés par une fonction dépendant seulement du nombre de variables et du discriminant de la forme.

J'ai obtenu ce résultat et l'ai exposé dans un cours de théorie des nombres à Strasbourg en 1954. Il ne semble pas avoir été remarqué antérieurement, quoique sa démonstration soit très simple et qu'il mette en évidence un caractère important de l'arithmétique des formes indéfinies.

Il a pour corollaire immédiat le "théorème du nombre fini de classes":

(B) Le nombre de classes arithmétiques de formes quadratiques indéfinies à n variables de discriminant donné, est fini. Et c'est probablement la démonstration la plus naturelle de ce théorème dû à Hermite.

Autre conséquence facile : t étant une constante réelle (positive, négative ou nulle) il existe une constante finie $\varphi(t)$ telle que, pour tout système de valeurs a_i, il existe un système d'entiers x_i, avec

$$t < f(x_1 - a_1, \dots, x_n - a_n) \leqslant \varphi(t)$$

φ étant fonction seulement de t, du nombre des variables et du discriminant de la forme quadratique indéfinie f, résultat dû à Blaney.

En outre les démonstrations fournissent des majorations explicites simples, meilleures en général que celles antérieurement connues dans les cas où le résultat n'est pas nouveau.

On pourrait appeler "de type compact" les classes algébriques de formes qui ont la propriété (A) (on définirait le discriminant d'une forme $p(x_1, \dots, x_n)$ de degré r, par $\left\{\text{Inf. disc (f)}\right\}^{r/2}$ pour toutes les formes quadratiques

définies positives majorant $|p|^{2/r}$). Automatiquement elles ont les propriétés (B) et (C) . Ainsi les formes "décomposables totalement réelles" sont aussi de type compact, cela résulte aisément d'un théorème connu de Siegel et Davenport.

2.- Résultats préliminaires sur les réseaux

Lemme de Grace.- Soit Π un parallélotope de R^n construit sur n vecteurs ℓ_h indépendants, $\Pi = \{ x = t_1 \ell_1 + \ldots + t_n \ell_n \; ; \; 0 \leq t_i \leq 1 \}$ si $a \in \Pi$ il existe un sommet s de Π avec $|s - a|^2 \leq \frac{1}{4} \sum \ell_h^2$.

(Ce lemme est implicite sous forme algébrique dans les calculs d'Hermite et de ses successeurs, mais souvent ignoré depuis. C'est dans Grace, Proc. London M.S. 1923, que j'en ai trouvé la première mention explicite.

J'en déduis par une construction récurrente

Théorème 1.- Soient $\ell_1 , \ldots , \ell_n$, n éléments indépendants d'un réseau G de R^n , rangés par grandeurs croissantes, $\ell_{h+1}^2 \geq \ell_h^2$. Il existe une base $a_1 , \ldots , a_n$ de G avec :

$$a_h^2 \leq \text{Max}\ (1 , \tfrac{h}{4})\ \ell_h^2 \ .$$

Rappelons le :

Théorème de Minkowski.- Dans un réseau G de R^n on peut trouver n éléments indépendants $\ell_1 , \ldots , \ell_n$ avec :

$$\Pi \ell_h^2 \leq \gamma(n)^n \ (\det(G))^2$$

où $\gamma(n)$ est la constante d'Hermite de la dimension n ($\gamma(n) < n$).

Remarquons que le théorème 1 entraine alors l'existence d'une base $a_1 , \ldots , a_n$ de G avec $\Pi a_h^2 \leq \frac{32}{3} \frac{n!}{4^n} \gamma(n)^n (\det(G))^2$. C'est une des façons les plus rapides d'obtenir une inégalité amenant au théorème du nombre fini de classes pour les formes positives. D'autre part, par une étude analogue, basée sur le lemme de Grace, j'ai montré antérieurement qu'on peut obtenir très facilement l'inégalité de Remak sur les formes définies positives réduites au sens de Minkowski (Cf. Exposé au Séminaire Châtelet, Février 1950, multigraphié).

Appelons équilatère un réseau de R^n ayant n éléments indépendants $\ell_1 , \ldots , \ell_n$ tels que $\ell_1^2 = \ell_2^2 = \ldots = \ell_n^2$ et que $x^2 \geq \ell_1^2$ pour tout

$x \in G$ et $\neq 0$, et ε -équilatère un réseau, si l'égalité précédente est remplacée par $\ell_h^2 \leqslant (1+\varepsilon)\,\ell_1^2$ ε étant un nombre $\geqslant 0$. En utilisant les résultats qui précèdent, on a alors :

Théorème 2.- Un réseau équilatère de R^n admet une base $a_1, \ldots, a_n$ avec

$$a_h^2 \leqslant \mathrm{Max}\ (1\ ,\ \frac{h}{4})\ \gamma(n)\ (\det(G))^{2/n}$$

Un réseau ε -équilatère admet une base $a_1, \ldots, a_n$ avec

$$a_h^2 \leqslant (1+\varepsilon)^{\frac{n-h-1}{n}}\ \mathrm{Max}\ (1\ ,\ \frac{h}{4})\ \gamma(n)\ \det(G)^{2/n}\ .$$

3.- Application aux formes indéfinies

Soit $\varphi(x) = \sum_{i=1}^{p} x_i^2 - \sum_{j=1}^{q} x_{p+j}^2$, $p+q=n$, $p^2+q^2>0$, toute forme quadratique indéfinie à n variables, de signature $(p\ ,\ q)$ pourra s'écrire $f(x) = \varphi(\tau(x))$, τ transformation linéaire (homogène) à n variables de déterminant $\neq 0$ et $\mathrm{disc}(f) = (\det(\tau))^2$.

Soit G le réseau de base $a_1 = \tau(e_1)$, ... , $a_n = \tau(e_n)$ (e_n vecteurs unités sur les axes), soit b_1 , ... , b_n une base quelconque de G , $g(x) = \varphi(x_1 b_1 + \ldots + x_n b_n)$ est arithmétiquement équivalente à f et on obtient ainsi toutes les formes de la classe de f . On dira que le réseau G représente la classe de f .

Soit Γ le groupe des automorphismes de φ (transformations linéaires (homogènes) laissant φ invariant). Si $G' = \xi(G)$ avec $\xi \in \Gamma$, G' représente évidemment la même classe de formes que G , nous dirons que G' est semblable à G (pour la "forme type" φ).

Théorème 2.- Tout réseau de R^2 est semblable (pour la forme type $\varphi = x_1^2 - x_2^2$) à un réseau équilatère. Tout réseau de R^n est semblable (par rapport à la forme type φ) à un réseau ε -équilatère, et cela quel que soit le choix a priori d'un $\varepsilon > 0$.

Pour $n=2$ le résultat est implicite dans la réduction continuelle d'Hermite pour les formes indéfinies binaires :

Soit $u = x_1 + x_2$, $v = x_1 - x_2$, S la transformation $u \longrightarrow u^2$ $v \longrightarrow v^2$ $H = S(G - \{0\})$, K la frontière de l'enveloppe convexe de H . K est une ligne polygonale ayant toujours au moins un, et en général une infinité de côtés de longueur finie. A chacun d'eux est associée une transformation

linéaire $\tau \in \Gamma$ telle que le réseau $G' = \tau(G)$ semblable à G, soit équilatère. K est l'analogue pour la réduction continuelle d'Hermite, de la ligne polygonale de Klein pour les fractions continues.

Pour $n > 2$ le résultat est implicite dans un travail de Rogers (Proceed. London Math. Soc. 1953) fait en vue de l'étude du "problème homogène" pour les formes indéfinies. En effet si $\mu(G) = \text{Min } x^2 (x \in G \ , \ x \neq 0)$

et $\nu(G) = \text{Sup } \mu(S(G)) \ (S \in \Gamma)$

soit S_r une suite d'éléments de Γ telle que $\mu(S_n(G)) \longrightarrow \nu(G)$ on peut extraire de S_r une suite partielle $S_{r'}$ telle que les réseaux $G'_r = S_{r'}(G)$ semblables à G, convergent vers un réseau G^* avec $\nu(G) = \nu(G^*) = \mu(G^*)$. Par un raisonnement facile de déformation, on voit que G^* est équilatère. Donc pour tout $\varepsilon > 0$, G est semblable à un réseau ε-équilatère. Si le réseau G est associé à une forme dont les rapports des coefficients sont rationnels, on voit aisément que parmi les G'_r il n'y en a qu'un nombre fini de distincts et que G^* est donc semblable à G.

Des théorèmes (1) et (2) suit donc, par un calcul facile, le théorème A sous la forme plus précise

Théorème. - Si $f(x_1 , \ldots , x_n)$ est une forme quadratique réelle indéfinie à n variables, de discriminant Δ, pour tout $\varepsilon > 0$, il existe une forme $g(x_1 , \ldots , x_n) = \sum \gamma_{hk} x_h x_k$, arithmétiquement équivalent à f, avec :

$$|\gamma_{h,k}| \leqslant \sqrt{\text{Max } (1 , \tfrac{h}{4}) \times \text{Max } (1 , \tfrac{k}{4})} \times \gamma(n) \times \Delta \times (1 + \varepsilon)$$

Pour une forme indéfinie quelconque si $n = 2$, et pour une forme indéfinie dont les rapports des coefficients sont rationnels si n quelconque, on peut prendre $\varepsilon = 0$.

Pour le réseau équilatère G quelque soit $p \in R^n$ l'ensemble $(x - p)^2 \leqslant \frac{n}{4} \mu(G)$, a fortiori l'ensemble $(x - p)^2 \leqslant \frac{n \gamma(n)}{4} (\det(G))^2$ contient des représentants de toutes les classes de R^n mod G d'où le théorème (C) dans le cas général par un calcul facile; en particulier nous démontrons : quel que soient les constantes réelles a_h et le nombre $\varepsilon > 0$ l'inégalité :

$$0 < f(x_1 - a_1 , \ldots , x_n - a_n) \leqslant \left(\frac{3 + 2\sqrt{2}}{4}\right) n \gamma(n) \operatorname{disc}(f)(1 + \varepsilon)$$

a une solution en x_h entiers.

4.- Autres classes algébriques de formes de type compact

Soit M une classe algébrique de formes, de forme type φ (à n variables, de degré r). Γ le groupe des automorphismes de φ. A une classe arithmétique $C \subset M$ est associé un réseau de R^n, défini à un automorphisme de f près et deux réseaux G et G' seront dits semblables (par rapport à Γ) si $G' = \tau(G)$ $\tau \in \Gamma$. On a le

Théorème. - Pour que la classe algébrique M soit de type compact, il faut et il suffit qu'il existe un $\varepsilon \geqslant 0$ tel que tout réseau de R^n soit semblable (par rapport à Γ) a un réseau ε-équilatère.

Soit $\varphi = x_1 \times x_2 \times \ldots \times x_n$ pour $n = 2$ (Hermite), $n = 3$ (Remak), $n = 4$ (Dyson), on sait que tout réseau de R^n est semblable à un réseau équilatère par rapport à $\Gamma(\varphi)$.

Pour n quelconque, on n'a pas démontré un tel résultat. Mais Siegel a démontré (Cf. article de Davenport, Acta Arithmetica 1938) qu'étant donné un système de n formes linéaires réelles $\ell_h(x_1, \ldots, x_n)$ de déterminant unité, il existe des constantes C_h avec $\prod C_h = \text{Cte}$ ne dépendant que de n, telles que les inégalités $0 < \ell_h(x_1, \ldots, x_n) \leq C_h$ n'aient pas de solution en entiers x_i. On en déduit immédiatement que le critère précédent est satisfait et par conséquent que la classe algébrique des formes " décomposables totalement réelles" à n variables, est de type compact.