I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le cours a porté sur la *formule de Siegel,* relative au nombre de représentations d'une forme quadratique par une autre. On s'est borné au cas le plus simple, celui où le corps de base est **Q**, et où les formes quadratiques sont positives non dégénérées (cf. C.L. Siegel, *Ges. Abh.,* vol. I, n° 20) ; le cas des formes indéfinies a été seulement mentionné sans démonstration.

On sait depuis les travaux de T. Tamagawa, M. Kneser et A. Weil (*circa* 1960) que l'énoncé de Siegel « équivaut » à dire que, si $m \neq 1$, le *nombre de Tamagawa* du groupe spécial orthogonal $\mathbf{SO}_m$ est égal à 2 (ou — ce qui est plus proche du point de vue de Siegel — que le nombre de Tamagawa du groupe orthogonal $\mathbf{O}_m$ est égal à 1). La vérification de cette équivalence est élémentaire, mais quelque peu pénible. Ses principes sont indiqués dans :

A. WEIL, *Sur la théorie des formes quadratiques,* Œuvres Sci., vol. II, [1962 a] ;

T. TAMAGAWA, *Adèles,* Proc. Symp. Pure Math. IX, A.M.S., 1966, p. 113-121 ;

M. KNESER, *Quadratischen Formen,* Notes polycopiées, Göttingen, 1974.

L'un des buts du cours a été de donner une démonstration détaillée de l'équivalence en question, ainsi que des applications numériques.

a) *Préliminaires : le jeu des deux groupes*

Soient G un groupe localement compact unimodulaire, et Γ (resp. Ω) un sous-groupe discret (resp. ouvert compact) de G. Soit $I \subset G$ un ensemble de représentants des doubles classes $\Omega x \Gamma$; si $x \in I$, notons Γ_x le groupe fini $\Omega \cap x \Gamma x^{-1}$. On a :

$$\text{(1)} \qquad \mathrm{vol}(G/\Gamma) = \sum_{x \in I} \mathrm{vol}(\Omega/\Gamma_x) = \mathrm{vol}(\Omega) \sum_{x \in I} 1/w(x),$$

où $w(x)$ désigne l'ordre de Γ_x.

(Dans les applications, G est un groupe adélique dont la composante archimédienne G_∞ est compacte, Γ est le groupe de ses points rationnels, et $\mathrm{vol}(G/\Gamma)$ est le nombre de Tamagawa. Le groupe Ω est le produit de G_∞ et des groupes de points « p-entiers » ; son volume est un produit de volumes locaux. Les doubles classes de G modulo Ω et Γ s'interprètent comme les classes d'un « genre » ; la somme des $1/w(x)$ est la *masse* du genre, au sens d'Eisenstein. La formule (1) exprime cette masse en termes du nombre de Tamagawa.)

Soit g un sous-groupe fermé de G, soit $\gamma = g \cap \Gamma$, et supposons que $\mathrm{vol}(g/\gamma)$ soit *fini*. Soit φ une fonction continue à support compact sur G/g, invariante par Ω. Si $x \in G$, on pose :

$$N_x(\varphi) = \sum_{y \in \Gamma/\gamma} \varphi(xy) ;$$

cette somme ne dépend que de la double classe de x modulo Ω et Γ. On note $\tilde{N}(\varphi)$ la moyenne pondérée des $N_x(\varphi)$ pour x parcourant I :

$$\tilde{N}(\varphi) = \Big(\sum_{x \in I} Nx(\varphi)/w(x) \Big) / \Big(\sum_{x \in I} 1/w(x) \Big).$$

Un calcul facile (basé sur A. Weil, *Adeles and Algebraic Groups*, § 2.4) montre que :

$$\text{(2)} \qquad \tilde{N}(\varphi) = \frac{\mathrm{vol}(g/\gamma)}{\mathrm{vol}(G/\Gamma)} \cdot \int_{G/g} \varphi(y) dy,$$

pourvu que les mesures invariantes choisies sur G, g et G/g soient compatibles.

(Dans les applications, g est un groupe adélique, $\mathrm{vol}(g/\gamma)$ est son nombre de Tamagawa, et l'intégrale de φ sur G/g se calcule comme produit de « densités locales ». La formule (2) permet le passage « Siegel » $\Leftrightarrow$ « Tamagawa ».)

b) *Enoncé de la formule de Siegel*

Soient S et T des **Z**-modules libres de rangs m et n (avec $m \geqslant n \geqslant 1$), munis de formes quadratiques positives non dégénérées, à valeurs dans **Z**. Soit $(S_x)_{x \in I}$ un système de représentants des classes du genre de S (réseaux

localement isomorphes à S). Pour tout $x \in I$, on note $w(x)$ l'ordre du groupe d'automorphismes de S_x. La masse du genre de S est :

$$\text{Masse(S)} = \sum_{x \in I} 1/w(x).$$

Soit $N(S_x,T)$ le nombre des plongements $T \to S_x$ qui sont compatibles avec les formes quadratiques de ces réseaux. On suppose que $N(S_x,T) \neq 0$ pour au moins un $x \in I$ (cela revient à exiger que T soit *localement* plongeable dans S). On note $\tilde{N}(S,T)$ la moyenne pondérée des $N(S_x,T)$:

$$\tilde{N}(S,T) = \Big(\sum_{x \in I} N(S_x,T)/w(x)\Big)/\text{Masse(S)}.$$

La *formule de Siegel* exprime $\tilde{N}(S,T)$ comme produit de termes locaux :

$$\tilde{N}(S,T) = c_{m-n}(c_m)^{-1}\, \alpha_\infty(S,T) \prod_p \alpha_p(S,T), \tag{3}$$

où :

$c_k = 1$ si $k \neq 1$ et $c_1 = 1/2$;

$\alpha_p(S,T)$ est la densité des plongements p-adiques de T dans S (cf. ci-dessous) ;

$\alpha_\infty(S,T)$ est l'analogue archimédien des $\alpha_p(S,T)$.

Précisons la définition de $\alpha_p(S,T)$ (cf. Siegel, *loc. cit.*) ; c'est la limite pour $r \to \infty$ du rapport $c.N(S,T;p^r)/p^{rd}$ où :

$c = 1/2$ si $m = n$ et $c = 1$ si $m \neq n$,

$d = mn - n(n+1)/2$,

$N(S,T;p^r)$ = nombre des homomorphismes $T/p^rT \to S/p^rS$ compatibles avec les produits scalaires de ces deux groupes.

Quant à $\alpha_\infty(S,T)$, c'est le produit du $A_\infty(S,T)$ de Siegel par la constante c. (Noter que $1/c$ est le nombre des composantes connexes de la « variété » Y des plongements de T dans S, et que $d = \dim Y$.)

Dans (3), le produit infini porte sur les nombres premiers p, rangés par ordre croissant. C'est un produit convergent ; il est même absolument convergent si $m \geqslant 3$ et $m - n \neq 2$.

Deux cas particuliers sont spécialement intéressants :

Le cas $T = S$

On a alors $\tilde{N}(S,S) = 1/\text{Masse(S)}$ et (3) donne la formule de Minkowski-Siegel :

$$\text{Masse(S)} = c_m \cdot \alpha_\infty(S,S)^{-1} \prod_p \alpha_p(S,S)^{-1}. \tag{4}$$

Le cas $n = 1$

Le réseau T est alors isomorphe à $\mathbf{Z}$, muni de la forme quadratique tX^2, avec t entier > 0, et $N(S_x,T)$ est le *nombre de représentations de t par* S_x.

c) *Démonstration de la formule* (3)

La démonstration originale de Siegel procède par récurrence sur $m = \dim S$. Elle comporte deux parties :

Partie arithmétique

Utilisant l'hypothèse de récurrence, Siegel montre que (3) est vraie *à un facteur près*, ce facteur ne dépendant que de S (et même seulement de $S_{\mathbf{Q}} = \mathbf{Q} \otimes S$), mais pas de T.

Ce résultat peut se déduire de la formule (2) de a) ci-dessus, en prenant :

G = groupe adélique du groupe orthogonal $\mathbf{O}_m$ (relatif à $S_{\mathbf{Q}}$) ;

Γ = groupe des points rationnels de G ;

$\Omega = G_\infty \times \prod_p G(S_p)$, où $G(S_p)$ est le groupe orthogonal du $\mathbf{Z}_p$-réseau $S_p = \mathbf{Z}_p \otimes S$;

g = groupe adélique du groupe orthogonal $\mathbf{O}_{m-n}$ (relatif à un module quadratique W tel que $W \oplus T_{\mathbf{Q}} \simeq S_{\mathbf{Q}}$) ;

γ = groupe des points rationnels de g ;

G/g = espace des plongements adéliques de T dans S ;

φ = fonction caractéristique de l'ensemble des plongements adéliques de T dans S qui appliquent T_p dans S_p pour tout p.

On munit G, g et G/g de leurs mesures de Tamagawa (avec facteurs correctifs dus à la non connexion du groupe orthogonal en dimension > 0). On vérifie que l'intégrale de φ sur G/g est égale au produit $\alpha_\infty(S,T) \prod_p \alpha_p(S,T)$, et que $\tilde{N}(\varphi) = \tilde{N}(S,T)$. On obtient (3), avec c_{m-n} et c_m remplacés respectivement par $\tau(\mathbf{O}_{m-n})$ et $\tau(\mathbf{O}_m)$, où τ désigne le nombre de Tamagawa. L'hypothèse de récurrence montre en outre que $\tau(\mathbf{O}_{m-n}) = c_{m-n}$; d'où la formule (3) *au facteur près* $\lambda = \tau(\mathbf{O}_m)/c_m$.

Partie analytique

Il s'agit de prouver que $\lambda = 1$. Pour cela, Siegel applique la formule (3) (avec le facteur λ) au cas $n = 1$, i.e. aux représentations d'un entier $t \geqslant 1$ par les formes S_x. Il somme les formules ainsi obtenues pour $t \leqslant X$ (avec certaines restrictions de congruences sur t), et compare le résultat aux esti-

mations asymptotiques (pour $X \to \infty$) fournies par un calcul de volume à la Gauss. Cette comparaison lui fournit la relation cherchée : $\lambda = 1$! (Les cas de basse dimension : $m = 2, 3, 4$ nécessitent des démonstrations spéciales.)

d) *Exemple : la forme quadratique* $\sum_{i=1}^{i=m} X_i^2$

On désire calculer Masse(I_m), où I_m est le réseau $\mathbf{Z}^m$ muni de la forme quadratique standard $\sum X_i^2$. Vu (4), cela revient à calculer les facteurs locaux $\alpha_\infty(I_m, I_m)$ et $\alpha_p(I_m, I_m)$. Seul le cas $p = 2$ crée quelques difficultés [signalons à ce sujet que les formules données par H. Hasse et reproduites par W. Magnus (*Math. Ann.*, 1937), M. Eichler (*Grundl. Math. Wiss.*, 63, 1962, § 25.4) et J.W.S. Cassels (*Acad. Press*, 1978, p. 377) sont incorrectes pour $m \geqslant 9$]. Lorsque m est *divisible par* 4, on trouve :

$$\text{Masse}(I_m) = (1 - 2^{-k})(1 + \varepsilon\, 2^{1-k}) \mid b_k . b_2 b_4 b_6 \ldots b_{2k-2} \mid / 2.k\,!,$$

où $k = m/2$, $\varepsilon = (-1)^{m/4}$ et les b_i sont les nombres de Bernoulli.

Il y a des formules analogues lorsque m n'est pas divisible par 4. Voir là-dessus J. Conway et N. Sloane, *Europ. J. Comb.*, 3, 1982, p. 219-231 (cf. aussi Ch. Ko, *Acta Arith.*, 3, 1939, p. 79-85). Le travail de Conway-Sloane contient également une table des valeurs de Masse(I_m) pour $m \leqslant 32$, ainsi qu'une détermination explicite des classes du genre pour $m \leqslant 23$. Ainsi, pour $m = 9$, il y a 2 classes, et la masse du genre est $17/2786918400$.

e) *Compléments*

Le cours s'est achevé par de brèves indications sur :

— la décomposition des entiers en sommes de 5 carrés, problème célèbre, résolu par Eisenstein en 1847, et mis au concours par l'Académie des Sciences de Paris en 1881, avec le succès que l'on sait ;

— le lien avec les formes modulaires, et notamment le fait que la moyenne pondérée des séries thêta d'un genre est une série d'Eisenstein (le cas $m = 3$, laissé ouvert par Siegel, vient d'être traité par R. Schulze-Pillot, Göttingen, 1983) ;

— la démonstration adélique de $\tau(\mathbf{O}_m) = 1$.

Séminaire

J.-P. Serre : *Majorations du nombre des points rationnels d'une courbe algébrique sur un corps fini* (7 exposés) ;

J. Œsterlé : *Choix optima dans la méthode des « formules explicites »* (1 exposé) ;

J. Œsterlé : *Nombres de Tamagawa, et groupes unipotents en caractéristique* p (6 exposés).

Publication

J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini* (*C.R.*, t. 296, sér. I, p. 397-402).

Missions

Exposés

— *Curves over finite Fields,* Durham (New Hampshire), juillet 1982 ; Oxford, novembre 1982 ;

— *Nombre de points des courbes sur les corps finis,* Bordeaux, octobre 1982 ; Marseille, décembre 1982 ;

— *Applications de l'hypothèse de Riemann,* Bordeaux, octobre 1982 ;

— *On the coefficients of the series* $\varphi^k(x) = \prod_{n=1}^{\infty} (1 - x^n)^k$, Londres, novembre 1982 ;

— *Kajdan's Property, and Groups acting on Trees,* Oxford, novembre 1982 ; Glasgow, juin 1983 ;

— *La théorie du corps de classes,* Marseille, décembre 1982 ;

— *Courbes de genre* 1 *et* 2 *sur les corps finis,* Bordeaux, mars 1983 ;

— *Groupes de Galois sur* **Q**, séminaire sur les groupes finis, Paris, mars 1983 ;

— *1983, a good Year for Number Theory,* Glasgow, juin 1983.

Fonctions

Président du Comité Consultatif pour le Congrès International des Mathématiciens de Varsovie (1979-1983).

Vice-président du Comité Exécutif de l'Union Mathématique Internationale (1983-...).

Vice-président du Comité National Français des Mathématiciens (1983-...).

Distinction

Doctorat *honoris causa* de l'Université de Glasgow, juin 1983.