I. SCIENCES MATHÉMATIQUES PHYSIQUES ET NATURELLES

Algèbre et géométrie

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

Le cours a complété celui de l'année précédente, consacré aux points rationnels des variétés algébriques. Il a comporté deux parties :

1. *Points entiers sur les courbes algébriques*

Soient K un corps de nombres algébriques, S un ensemble fini de places de K contenant les places à l'infini, et A_S l'anneau des S-entiers de K.

1.1. *Le théorème de Siegel*

Soit X une K-variété affine, d'anneau de coordonnées R_X, et soit X(K) l'ensemble des K-points de X. Une partie M de X(K) est dite *quasi-entière* (relativement à l'anneau A_S) si, pour tout $f \in R_X$, le sous-A_S-module de K engendré par f(M) est de type fini. Il revient au même de dire qu'il existe un plongement affine de X dans lequel les coordonnées des points de M appartiennent à A_S (de sorte que les points de M sont « S-entiers »).

Si X est une *courbe* irréductible, le théorème de Siegel (généralisé par Mahler, LeVeque et Lang) dit qu'un tel ensemble M est *fini,* mis à part le cas exceptionnel où X est de genre 0, et a au plus 2 points (géométriques) à l'infini — auquel cas la normalisée de X est isomorphe à une droite ou à

une conique affine. La démonstration repose sur un théorème de « mauvaise approximation » pour les points algébriques des variétés abéliennes, théorème qui lui-même se déduit du théorème de Roth sur l'approximation des nombres algébriques. Le théorème de Siegel, comme celui de Roth, est *ineffectif* : il ne permet pas de trouver à coup sûr les points « S-entiers » d'une courbe donnée. (La présentation usuelle de cette démonstration fait également usage du théorème de Mordell-Weil, autre source d'ineffectivité. On peut s'en passer : cela a été prouvé il y a quelques années par Robinson et Roquette au moyen de « l'Analyse non standard », et cela peut se vérifier sans difficulté par des méthodes « standard ».)

1.2. *La méthode de Baker*

Moins générale que celle de Siegel, cette méthode a le grand avantage d'être *effective*. Elle s'applique notamment dans les cas suivants :

(a) courbe affine de genre 0, ayant au moins 3 points à l'infini ;

(b) courbe affine de genre 1 ;

(c) courbe hyperelliptique affine ayant au moins un point à l'infini dont le symétrique (pour l'involution canonique) est aussi à l'infini.

(Par contre, j'ignore si la méthode de Baker s'applique à une courbe affine de genre 2 ne satisfaisant pas à (c) ci-dessus.)

Le cas (a) se ramène à la résolution de l'équation

$$Ax + By + C = 0 \qquad \text{(avec } A, B, C \in \mathrm{A_S} \text{ donnés)}$$

où les inconnues x, y sont des éléments inversibles de $\mathrm{A_S}$. Il se traite en appliquant directement les minorations de Baker sur les combinaisons linéaires de logarithmes. Les cas (b) et (c) se ramènent au cas (a) par les arguments « fonctoriels » suivants :

(i) Si $X \to Y$ est un morphisme de variétés affines, à fibres finies, et si le théorème de finitude est vrai pour Y, il l'est aussi pour X.

(ii) Si $X \to Y$ est un morphisme fini, étale et surjectif de variétés affines, et si le théorème de finitude est vrai pour X (et pour toute extension finie de K), il l'est aussi pour Y.

1.3. *Applications aux courbes elliptiques*

La méthode de Baker, appliquée à l'équation $Y^2 - X^3 = D$, donne la finitude (effective) des courbes elliptiques sur K ayant bonne réduction en dehors d'un ensemble fini donné de places (théorème de Šafarevič). Ce résultat peut lui-même être utilisé pour prouver l'irréductibilité des modules de Tate d'une courbe elliptique sans multiplications complexes (cf. cours 1965/1966).

1.4. *Applications aux corps quadratiques imaginaires de nombre de classes égal à 1* (Heegner-Stark-Baker)

A un tel corps est associée une courbe elliptique à multiplications complexes, définie sur **Q**, dont l'invariant modulaire appartient à **Z**. De là on déduit des points entiers de diverses courbes modulaires, et notamment des courbes X_N attachées aux normalisateurs de sous-groupes de Cartan non déployés de niveau N, pour N convenable. En choisissant N de telle sorte que le théorème de finitude de Siegel s'applique à X_N (et soit effectif), on en déduit la détermination des corps en question. Divers choix de N sont possibles : Heegner et Stark prennent $N = 24$; Siegel (*Ges. Abh.*, 85) prend $N = 15$; on peut aussi utiliser $N = 7$, qui conduit à des unités « exceptionnelles » (au sens de Nagell) du corps cubique réel de discriminant 49 ; même chose pour $N = 9$.

2. *Le théorème d'irréductibilité de Hilbert*

2.1. *Ensembles minces*

Soit K un corps, que l'on suppose de caractéristique 0 pour simplifier. Une partie Ω de $\mathbf{P}_n(K)$ est dite *mince* s'il existe un morphisme de variétés algébriques $\varphi : X \to \mathbf{P}_n$, défini sur K, tel que :

(a) Ω est contenu dans $\varphi(X(K))$;

(b) $\dim X \leqslant n$;

(c) il n'existe pas d'application rationnelle de $\mathbf{P}_n$ dans X qui soit une section de φ.

(Un cas typique où (b) et (c) sont vérifiés est celui où X est un revêtement (ramifié) irréductible de $\mathbf{P}_n$, de degré $\geqslant 2$.)

Cette définition s'applique également aux parties de l'espace affine K^n, considérées comme plongées dans l'espace projectif $\mathbf{P}_n(K)$. Ainsi, pour $n = 1$, l'ensemble des carrés est une partie mince de K, de même que l'ensemble des cubes, etc.

2.2. *Propriétés élémentaires des ensembles minces*

(a) Si K_1 est une extension finie de K, et si Ω_1 est une partie mince de $\mathbf{P}_n(K_1)$ (relativement à K_1), alors $\Omega_1 \cap \mathbf{P}_n(K)$ est une partie mince de $\mathbf{P}_n(K)$.

(b) Soit Ω une partie mince de $\mathbf{P}_n(K)$. Il existe un ouvert dense U de l'espace projectif dual tel que, pour tout hyperplan $H \in U(K)$, l'ensemble $\Omega \cap H(K)$ soit mince dans $H(K) \simeq \mathbf{P}_{n-1}(K)$. Cela résulte du théorème de Bertini.

(c) Soit

$$F(X, T_1, ..., T_n) = a_0(T) + a_1(T)X + ... + a_r(T)X^r$$

un polynôme irréductible de degré r, à coefficients dans le corps de fonctions rationnelles $K(T_1, ..., T_n)$. Il existe une partie mince Ω_F de K^n telle que, si $t = (t_1, ..., t_n)$ n'appartient pas à Ω_F, le polynôme spécialisé

$$F_t(X) = a_0(t) + a_1(t)X + ... + a_r(t)X^r$$

soit irréductible de degré r, et ait même groupe de Galois sur K que $F(X, T)$ sur $K(T)$.

d) Soient Z une variété K-irréductible et $f : Z \to \mathbf{P}_n$ un morphisme. L'ensemble des points $t \in \mathbf{P}_n(K)$ dont la fibre $f^{-1}(t)$ n'est pas K-irréductible est mince.

2.3. *Corps hilbertiens*

Un corps K est dit hilbertien si, pour tout $n \geqslant 1$, l'ensemble $\mathbf{P}_n(K)$ n'est pas mince ; vu 2.2.(b), il suffit d'ailleurs de le vérifier pour $n = 1$.

Si K est hilbertien, et si K_1 est une extension finie de K, le corps K_1 est hilbertien (la réciproque est inexacte).

Un corps algébriquement clos n'est pas hilbertien ; il en est de même d'un corps p-adique.

Tout corps de la forme $k(T)$ est hilbertien.

2.4. *Le théorème de Hilbert*

Ce théorème affirme que *tout corps de nombres algébriques* (fini sur $\mathbf{Q}$) *est hilbertien ;* vu 2.3., il suffit d'ailleurs de le vérifier pour $\mathbf{Q}$; dans ce cas, il revient à dire que tout sous-ensemble mince de $\mathbf{Q}$ est distinct de $\mathbf{Q}$.

Il existe de nombreuses démonstrations de ce théorème ; le cours en a exposé trois ou quatre. Les plus intéressantes précisent la « petitesse » des ensembles minces, cf. ci-dessous.

2.5. *Ensembles minces : cas* $n = 1$

Soit Ω une partie mince de $\mathbf{P}_1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$. On va voir en quel sens on peut dire que Ω contient « peu » de points rationnels, et « peu » de points entiers.

(a) *Points rationnels*

Si x est $\geqslant 1$, notons $M(x)$ (resp. $M_\Omega(x)$) le nombre des points $P \in \mathbf{P}_1(\mathbf{Q})$

(resp. $P \in \Omega$) dont la hauteur $H(P)$ est $\leqslant x$. On a

$$M(x) \sim 12x^2/\pi^2 \qquad \text{pour } x \to \infty,$$

alors que $M_\Omega(x)$ est au plus de l'ordre de la *racine carrée* de $M(x)$:

$$M_\Omega(x) = O(x) \qquad \text{pour } x \to \infty.$$

(Cela résulte des propriétés des hauteurs des points rationnels des courbes algébriques.)

(b) *Points entiers*

Notons $N_\Omega(x)$ le nombre des $P \in \Omega \cap \mathbf{Z}$ tels que $|P| \leqslant x$. On a

$$N_\Omega(x) = O(x^{1/2}) \qquad \text{pour } x \to \infty.$$

(Cela résulte du théorème de Siegel, cf. § 1.)

En particulier, il existe une *infinité de nombres premiers* (ou de sommes de deux carrés) n'appartenant pas à Ω.

2.6. *Ensembles minces : cas général*

Soit Ω une partie mince de $\mathbf{P}_n(\mathbf{Q})$, avec $n \geqslant 1$. Définissons $M(x)$ et $N_\Omega(x)$ comme ci-dessus. On a alors :

(a) $M_\Omega(x) = O(x^{n+1/2} \log x) \qquad$ pour $x \to \infty$

et

(b) $N_\Omega(x) = O(x^{n-1/2} \log x) \qquad$ pour $x \to \infty$.

(On peut d'ailleurs remplacer le terme $\log x$ par $(\log x)^\gamma$, avec $\gamma < 1$ dépendant de Ω.)

L'énoncé (a) se déduit de (b), appliqué au cône sur Ω (dans l'espace affine de dimension $n+1$) ; il n'est pas certain que l'exposant $n + 1/2$ qui y figure soit optimal : peut-être est-il possible de le remplacer par n ? Par contre, (b), qui est dû à S.D. Cohen (*Proc. London Math. Soc.*, 1981) est essentiellement optimal.

Le principe de la démonstration de (b) est le suivant. On décompose d'abord Ω comme réunion finie d'ensembles minces « élémentaires » Ω_i jouissant de la propriété suivante :

(*) il existe une constante $c_i < 1$ et un ensemble frobénien Π_i de nombres premiers, de densité > 0, tels que, pour tout $p \in \Pi_i$, l'image de Ω_i dans $(\mathbf{Z}/p\mathbf{Z})^n$ par réduction (mod p) ait au plus $c_i p^n$ éléments.

(Cela se fait en appliquant le théorème de Lang-Weil sur le nombre de points (mod p) d'une variété algébrique.)

Le théorème du *grand crible* (à n variables) permet alors de passer de (*) à (b) ci-dessus. Il y a des résultats analogues sur un corps de nombres quelconque.

Signalons une application de (a) :

(c) Si X est une sous-variété irréductible de $\mathbf{P}_N$ de dimension $n < N$ et de degré $d \geqslant 2$, et si $M_X(x)$ désigne le nombre des points $P \in X(\mathbf{Q})$ tels que $H(P) \leqslant x$, on a

$$M_X(x) = O(x^{n+1/2} \log x) \qquad \text{pour } x \to \infty.$$

Ici encore, il est probable que l'exposant $n + 1/2$ n'est pas optimal.

2.7. *Applications du théorème d'irréductibilité de Hilbert*

(i) *Construction d'extensions de* **Q** *de groupe de Galois donné*

On utilise 2.2.(c) qui montre que l'on peut « spécialiser » des paramètres sans toucher au groupe de Galois. Hilbert en donne pour exemple l'équation

$$X^n - X = t \qquad (t \in \mathbf{Q})$$

qui est irréductible et de groupe de Galois $\mathfrak{S}_n$ pour tout t non contenu dans un ensemble mince dépendant de n.

Cette méthode n'a malheureusement pas encore abouti à démontrer ce que certains espèrent, à savoir que *tout groupe fini* est groupe de Galois d'une extension de **Q**. La liste des groupes pour lesquels cette propriété a été démontrée est en fait très restreinte ; parmi les groupes simples non abéliens, il n'y a guère que les groupes alternés et les groupes $\mathbf{PSL}_2(\mathbf{F}_p)$ lorsque $(\frac{2}{p}) = -1$, $(\frac{3}{p}) = -1$ ou $(\frac{7}{p}) = -1$ (K. Shih) ; on ignore ce qu'il en est pour les groupes de Mathieu, par exemple (sans parler des autres groupes sporadiques...).

(ii) *Construction de courbes elliptiques sur* **Q** *de rang 9 et 10* (d'après A. Néron)

Soit A une variété abélienne sur le corps $K = \mathbf{Q}(T_1, ..., T_n)$ et soit A(K) le groupe des K-points de A. Dans sa thèse, Néron a prouvé :

(a) A(K) est un groupe de type fini ;

(b) il existe un ensemble mince Ω_A de $\mathbf{Q}^n$ tel que, si $t = (t_1, ..., t_n)$ appartient à $\mathbf{Q}^n - \Omega_A$, la variété abélienne A_t « spécialisée » de A en t contient un groupe de points rationnels isomorphe à A(K) ; en particulier, on a rang $A_t(\mathbf{Q}) \geqslant$ rang A(K).

Ainsi, pour construire des courbes elliptiques sur $\mathbf{Q}$ de rang $\geqslant r$ (avec r donné), il suffit de résoudre le problème analogue sur le corps $\mathbf{Q}(T_1, ..., T_n)$. Néron a montré que c'est possible pour $r = 9$ et $r = 10$, et il a esquissé une méthode qui devrait donner $r = 11$; le cas $r \geqslant 12$ reste ouvert.

Séminaire

Jean-Jacques Sansuc, *Hauteurs canoniques et nombres de Tamagawa,* d'après S. Bloch, *Invent. Math.* 58 (1980), p. 65-76 (deux exposés).

Publications

J.-P. Serre, *Extensions icosaédriques* (*Sém. de Th. des Nombres,* 1979-1980, Bordeaux, exposé 19, 7 pages).

— *Deux lettres* (*Mémoires S.M.F.,* 2e série, n° 2, 1980, p. 95-102).

Missions

Exposés :

— *Arithmetic of elliptic curves,* Stockholm, septembre 1980 ;

— *Poids et Racines,* E.N.S.J.F., Montrouge, décembre 1980 ;

— *Sieves and Modular Forms,* Oberwolfach, décembre 1980 ; Cambridge, janvier 1981 ;

— *Représentations ℓ-adiques,* Séminaire Delange-Pisot-Poitou, janvier 1981 ;

— *Réduction* (mod p^n) *des variétés p-adiques,* Marseille, mai 1981 ; Séminaire Delange-Pisot-Poitou, juin 1981 ; Londres, juin 1981 ;

— *La fonction de Ramanujan,* Berne, mai 1981 ; Londres, juin 1981.

Distinction

Doctorat *honoris causa* de l'Université de Stockholm, septembre 1980.