I. SCIENCES MATHÉMATIQUES PHYSIQUES ET NATURELLES

Algèbre et géométrie

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

Le sujet du cours a été l'étude des points rationnels des variétés algébriques, et plus spécialement des variétés abéliennes et des courbes algébriques : hauteurs, théorème de Mordell-Weil et conjecture de Mordell.

Il a comporté quatre parties :

1. *Hauteurs*

Hauteurs sur l'espace projectif

Soit $x \in \mathbf{P}_n(\mathbf{Q})$ un point rationnel de l'espace projectif $\mathbf{P}_n$ de dimension n. Choisissons les coordonnées projectives $(x_0, ..., x_n)$ de x de telle sorte que l'on ait :

$$x_i \in \mathbf{Z} \text{ pour tout } i \qquad \text{et} \qquad \text{pgcd}(x_0, ..., x_n) = 1 ;$$

un tel choix existe, et est unique à un changement de signe près.

La *hauteur* $\mathrm{H}(x)$ du point x est alors définie par :

$$\mathrm{H}(x) = \mathrm{Sup}(|x_0|, ..., |x_n|).$$

La fonction H se prolonge de façon naturelle aux *points algébriques* de $\mathbf{P}_n$, autrement dit aux éléments de $\mathbf{P}_n(\overline{\mathbf{Q}})$. Si $x = (x_0, ..., x_n)$ est un tel point, et si les x_i appartiennent à un sous-corps K de $\overline{\mathbf{Q}}$ de degré fini sur $\mathbf{Q}$, on a :

$$\mathbf{H}(x) = \prod_v \mathrm{Sup}_i |x_i|_v^{1/d}, \text{ avec } d = [\mathbf{K} : \mathbf{Q}],$$

où v parcourt l'ensemble des places de K, et $|x_i|_v$ désigne le « module » de x_i dans le corps localement compact K_v complété de K en v (Bourbaki, INT VII, § 1, n° 10). On a $H(x) \geqslant 1$. On pose :

$$h(x) = \log H(x) ;$$

c'est la *hauteur logarithmique* du point x.

Théorème de finitude

Appelons *degré* d'un point $x = (x_0, ..., x_n)$ de $\mathbf{P}_n(\overline{\mathbf{Q}})$ le degré de l'extension de $\mathbf{Q}$ engendrée par les x_i/x_j avec $x_j \neq 0$. D'après un théorème de D.G. Northcott, les points de $\mathbf{P}_n(\overline{\mathbf{Q}})$ de degré d donné et de hauteur bornée sont *en nombre fini* : pour $d = 1$ c'est immédiat, et le cas général se ramène à celui-là grâce à un produit symétrique d-uple. En particulier, si K est un sous-corps de $\overline{\mathbf{Q}}$ de degré fini d, et si X est un nombre réel, les points de $\mathbf{P}_n(K)$ de hauteur $\leqslant X$ sont en nombre fini ; soit $N_{K,n}(X)$ leur nombre. Le comportement de $N_{K,n}(X)$ pour $X \to \infty$ a été déterminé par S. Schanuel (*Bull. Soc. math. France,* 107, 1979, p. 433-449). Le résultat est le suivant :

$$N_{K,n}(X) = c_{K,n} X^{d(n+1)} + \begin{cases} O(X \log X) & \text{si } d = n = 1 \\ O(X^{d(n+1)-1}) & \text{sinon} \end{cases}$$

où $c_{K,n}$ est une constante > 0 ne dépendant que de K et de n. On a en particulier :

$$N_{K,n}(X) \asymp X^{d(n+1)} \quad \text{pour } X \to \infty.$$

Il serait intéressant d'avoir des résultats analogues pour d'autres variétés que les espaces projectifs.

Hauteurs sur les variétés projectives

Soit V une variété projective sur $\overline{\mathbf{Q}}$, et soit Pic (V) le groupe des classes de fibrés vectoriels de rang 1 sur V (i.e. le groupe des classes de « diviseurs de Cartier » de V). Si $\varphi : V \to \mathbf{P}_n$ est un morphisme de V dans un espace projectif nous noterons $c(\varphi)$ l'élément de Pic (V) image réciproque par φ du générateur standard de Pic $(\mathbf{P}_n)$.

Soit $c \in$ Pic (V). On peut écrire c sous la forme :

$$c = c(\varphi) - c(\psi)$$

où φ et ψ sont des morphismes de V dans des espaces projectifs convenables. Choisissons un tel couple (φ, ψ), et notons h_φ et h_ψ les fonctions sur $V(\overline{\mathbf{Q}})$ définies par :

$$h_\varphi(x) = h(\varphi(x)) \quad \text{et} \quad h_\psi(x) = h(\psi(x)) \quad (x \in V(\overline{\mathbf{Q}})).$$

D'après un théorème de Weil et Néron, la fonction $h_\varphi - h_\psi$ ne dépend

que de c, à l'addition près d'une fonction bornée sur $V(\overline{\mathbf{Q}})$, autrement dit « à $O(1)$ près ». On peut donc poser :

$$h_c = h_\varphi - h_\psi ;$$

c'est la *fonction hauteur* (logarithmique) relative à c ; elle est définie modulo $O(1)$. Ses principales propriétés sont :

a) (Additivité) $h_{c+d} = h_c + h_d + O(1)$ si $c, d \in \mathrm{Pic}(V)$.

b) (Fonctorialité) $h_{c'} = h_c \circ f + O(1)$ si $f : V' \to V$ est un morphisme, et si $c \in \mathrm{Pic}(V)$, $c' \in \mathrm{Pic}(V')$ et $c' = f^*(c)$.

c) (Positivité) Soit F_c l'intersection des supports des diviseurs positifs appartenant à la classe c. La restriction de h_c au complémentaire de F_c est minorée (i.e. positive modulo $O(1)$).

d) Si c est ample, h_c tend vers $+\infty$ sur les points de degré borné, et l'on a $h_d = O(1 + h_c)$ pour tout $d \in \mathrm{Pic}(V)$.

e) Si V est non singulière, on a $h_c = O(1)$ si et seulement si c appartient au sous-groupe de torsion de Pic (V).

f) Si V est non singulière, si c est ample, et si $d \in \mathrm{Pic}(V)$ est numériquement équivalent à 0, on a $h_d = O(1 + h_c^{1/2})$.

Les démonstrations de a), b), c) et d) sont faciles. Celles de e) et f) utilisent certains des résultats de Néron résumés ci-dessous.

2. *Hauteurs normalisées*

La normalisation des hauteurs est due à A. Néron. Elle consiste, lorsque V est une variété abélienne, à définir des *représentants canoniques* $\hat{h}_c$ des h_c qui éliminent les « $O(1)$ » de la théorie générale. Comme l'a montré J. Tate, on peut baser la construction des $\hat{h}_c$ sur le résultat élémentaire suivant :

Lemme - *Soient* S *un ensemble et* $\pi : S \to S$ *une application. Soit* f *une fonction sur* S *telle que* $f \circ \pi = kf + O(1)$, *avec* $|k| > 1$. *Il existe alors une fonction* $\hat{f}$ *sur* S *et une seule fonction telle que :*

$$\hat{f} = f + O(1) \text{ , } \textit{et} \quad \hat{f} \circ \pi = k\hat{f} .$$

(Démonstration : définir $\hat{f}(x)$ comme $\lim k^{-n} f(\pi^n x)$ pour $n \to \infty$.)

Soient alors A une variété abélienne sur $\overline{\mathbf{Q}}$ et c un élément de Pic (A). Supposons que c soit *symétrique* (resp. *antisymétrique*), autrement dit soit invariant (resp. anti-invariant) par l'involution $x \mapsto -x$ de A. Le lemme ci-dessus s'applique à $S = A(\overline{\mathbf{Q}})$, $f = h_c$, $\pi(x) = 2x$ et $k = 4$ (resp. $k = 2$). Cela définit $\hat{h}_c$ lorsque c est, soit symétrique, soit antisymétrique ; le cas général s'en déduit par linéarité. Les hauteurs canoniques $\hat{h}_c$ jouissent des propriétés suivantes :

a) $\hat{h}_{c+d} = \hat{h}_c + \hat{h}_d$ si $c, d \in \mathrm{Pic}(A)$.

b) $\hat{h}_{c'} = \hat{h}_c \circ f$ si $f : B \to A$ est un homomorphisme de variétés abéliennes (avec $f(0) = 0$) et si $c \in \mathrm{Pic}(A)$, $c' \in \mathrm{Pic}(B)$ et $c' = f^*(c)$.

c) $\hat{h}_c = 0$ si et seulement si c est d'ordre fini dans $\mathrm{Pic}(A)$.

d) Si c est antisymétrique, $\hat{h}_c$ est additive, et se prolonge en une forme linéaire sur $\mathbf{R} \otimes A(\overline{\mathbf{Q}})$.

e) Si c est symétrique, $\hat{h}_c$ est quadratique, et se prolonge en une forme quadratique sur $\mathbf{R} \otimes A(\overline{\mathbf{Q}})$; si de plus c est ample, on a $\hat{h}_c(x) > 0$ pour tout élément $x \neq 0$ de $\mathbf{R} \otimes A(\overline{\mathbf{Q}})$.

Dualité

Soit A′ la variété abélienne duale de A, et soit $P \in \mathrm{Pic}(A \times A')$ la classe du *diviseur de Poincaré* de $A \times A'$ (normalisée de telle sorte que ses restrictions à A et A′ soient nulles). La hauteur canonique $\hat{h}_P$ associée à P est une forme bilinéaire sur $A(\overline{\mathbf{Q}}) \times A'(\overline{\mathbf{Q}})$, appelée *forme de Néron*. La connaissance de cette forme entraîne celle de toutes les hauteurs canoniques $\hat{h}_c$: :

si $c \in \mathrm{Pic}(A)$ est antisymétrique, c est algébriquement équivalent à 0 et on peut l'identifier grâce à P à un élément de $A'(\overline{\mathbf{Q}})$; on a :

$$\hat{h}_c(x) = \hat{h}_P(x, c) \quad \text{pour tout } x \in A(\overline{\mathbf{Q}}) ;$$

si $c \in \mathrm{Pic}(A)$ est symétrique, on a :

$$\hat{h}_c(x) = -\tfrac{1}{2}\hat{h}_P(x, \varphi_c(x)) \quad \text{pour tout } x \in A(\overline{\mathbf{Q}}),$$

où φ_c est l'homomorphisme de A dans A′ défini par c.

Décomposition de $\hat{h}_c$ en somme de termes locaux

Néron a donné une telle décomposition. Le cours s'est borné à résumer ses résultats, en insistant sur le cas où A est une courbe elliptique (i.e. dim A = 1). Dans ce cas, en effet, J. Tate a donné des procédés de calcul effectifs pour les composantes locales en question ; voir là-dessus S. Lang, *Elliptic Curves - Diophantine Analysis* (Springer-Verlag, 1978) ainsi que H. Zimmer, *J. Crelle*, 307/308 (1979), p. 221-246.

Malgré ces procédés de calcul, la nature arithmétique des $\hat{h}_c(x)$ reste mystérieuse. On ignore par exemple si $\hat{h}_c(x)$ peut être un nombre algébrique $\neq 0$ (cela paraît peu probable).

3. *Le théorème de Mordell-Weil*

Enoncé et principe de démonstration

Soient K un sous-corps de $\overline{\mathbf{Q}}$ de degré fini sur $\mathbf{Q}$, A une variété abélienne définie sur K, et $\Gamma = A(K)$ le groupe des K-points de A. Le théorème de Mordell-Weil dit que Γ est un groupe *de type fini.*

Pour le démontrer, on prouve d'abord l'assertion plus faible suivante :

(*) - *Si n est un entier $\neq 0$, le groupe $\Gamma/n\Gamma$ est fini.*

La démonstration de (*) peut se faire par diverses méthodes. On peut utiliser le théorème de Chevalley-Weil sur les extensions non ramifiées. On peut aussi plonger $\Gamma/n\Gamma$ dans un groupe de cohomologie $H^1(K, A_n)$ et utiliser la finitude de l'ensemble des éléments de ce groupe qui sont non ramifiés en dehors d'un nombre fini de places. Il est également possible, en suivant une idée de Honda, de déduire (*) du fait général suivant : si $\varphi : G_1 \to G_2$ est une isogénie de groupes algébriques, l'image par φ d'un sous-groupe arithmétique de G_1 est un sous-groupe arithmétique de G_2.

Une fois (*) démontrée pour un $n \geqslant 2$, un argument de descente à la Fermat, utilisant la théorie des hauteurs, permet d'en déduire que Γ est de type fini. (Variante : montrer, grâce aux hauteurs canoniques, que Γ est somme directe d'un groupe fini et d'un groupe libre, lequel est nécessairement de type fini à cause de (*).)

Application : nombre de points rationnels de hauteur $\leqslant X$

Choisissons un plongement φ de A dans un espace projectif $\mathbf{P}_n$. Si X est un nombre réel, notons $N_{K,A}(X)$ le nombre des points $x \in A(K)$ tels que $H(\varphi(x)) \leqslant X$. On a :

$$\log H(\varphi(x)) = h_\varphi(x) = \hat{h}_{c(\varphi)}(x) + O(1),$$

et $\hat{h}_{c(\varphi)}$ est une forme quadratique positive. On déduit de là l'estimation suivante, due à Néron :

$$N_{K,A}(X) = \lambda (\log X)^{r/2} + O((\log X)^{(r-1)/2}) \quad \text{pour } X \to \infty,$$

où r est le rang de A (K) et λ un nombre > 0.

En particulier, $N_{K,A}(X)$ est de l'ordre de grandeur de $(\log X)^{r/2}$: une variété abélienne a « beaucoup moins de points » qu'un espace projectif.

Problèmes

Le théorème de Mordell-Weil n'est qu'un théorème d'existence. Il soulève de nombreuses questions. Notamment :

a) Peut-on déterminer *effectivement* un ensemble fini engendrant A(K) ? En particulier, peut-on calculer effectivement le *rang* de ce groupe ? (La démonstration de (*) ne donne qu'une majoration du rang.)

Lorsque $K = \mathbf{Q}$ et $\dim A = 1$, Y. Manin a montré que ces questions auraient une réponse affirmative si l'on admettait les conjectures de Birch-Swinnerton-Dyer et de Taniyama-Weil (ce qui est beaucoup demander...).

b) Quelle est la structure de $A(\overline{\mathbf{Q}})$ comme module galoisien sur $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$? En particulier, comment varie le rang de A(K) lorsque l'on agrandit le corps K ? (Des exemples intéressants de telles variations ont été donnés par B. Mazur et M. Harris.)

c) Fixons K ainsi que la dimension de A (par exemple $\dim A = 1$). Est-il vrai que l'ordre du sous-groupe de torsion de A(K) ait une borne indépendante de A ? (C'est vrai pour $K = \mathbf{Q}$ et $\dim A = 1$, d'après un théorème de B. Mazur.) Le rang de A(K) peut-il être arbitrairement grand ? (Il y a là-dessus des résultats de Néron datant de 1952 et 1954 sur lesquels on reviendra dans le cours de 1980/1981.)

4. *La conjecture de Mordell*

Enoncé et généralisations

Soient K un sous-corps de $\overline{\mathbf{Q}}$ de degré fini sur $\mathbf{Q}$, et C une courbe algébrique (projective, lisse, absolument connexe) définie sur K. On suppose que le *genre* g de C est $\geqslant 2$ (ce qui élimine les courbes rationnelles et les courbes elliptiques). La conjecture de Mordell est l'assertion suivante :

($M_?$) - *L'ensemble* C(K) *des* K*-points de* C *est fini.*

Choisissons un diviseur D de degré 1 sur la courbe C (ce qui est possible si C(K) est non vide), et faisons correspondre à tout point x de C la classe du diviseur $(x) - D$, qui est de degré 0. On obtient ainsi un plongement de C dans sa jacobienne J, qui est une variété abélienne de dimension g. Si l'on identifie C à une courbe de J par ce plongement, on a :

$$C(K) = C(\overline{\mathbf{Q}}) \cap \Gamma,$$

où $\Gamma = J(K)$ est le groupe des K-points de J. D'après le théorème de Mordell-Weil, Γ est un groupe de type fini. On peut donc reformuler la conjecture de Mordell de la manière suivante :

($M_?$) - *L'intersection de* $C(\overline{\mathbf{Q}})$ *et d'un sous-groupe de type fini de* $J(\overline{\mathbf{Q}})$ *est finie.*

S. Lang a proposé la généralisation suivante de (M_7) :

(M_{77}) - *Si* C *est plongée dans une variété abélienne* A *définie sur une extension* L *de* K, *et si* Λ *est un sous-groupe de* A(L) *tel que* $\mathbf{Q} \otimes \Lambda$ *soit de rang fini sur* $\mathbf{Q}$, *alors l'intersection de* C(L) *et de* Λ *est finie.*

(Noter qu'on ne suppose pas que Λ soit de type fini.)

Le cas où Λ est le sous-groupe de torsion A_t de A(L) avait déjà été signalé par Y. Manin et D. Mumford. Ce cas n'est pas encore résolu. Toutefois, F. Bogomolov vient d'obtenir un résultat partiel encourageant : il a prouvé la finitude de $C(L) \cap \Lambda$ lorsque Λ est somme directe d'un nombre fini de composantes p-primaires de A_t.

Démonstration de la conjecture de Mordell dans des cas particuliers

On sait prouver la finitude de C(K) lorsqu'on fait l'une des hypothèses suivantes :

i) (C. Chabauty) *Le rang de* $\Gamma = J(K)$ *est* $< g$.

ii) (V. Dem'janenko et Y. Manin) *Il existe une variété abélienne* A *définie sur* K *telle que* $\operatorname{rang} \operatorname{Hom}_K(J, A) > \operatorname{rang} A(K)$.

Le cas i) se traite par une méthode p-adique à la Skolem ; le cas ii) utilise la théorie des hauteurs canoniques.

Signalons une application de ii) due à Manin : si p est un nombre premier, il existe un entier $n_0 = n_0(K, p)$ tel que la courbe modulaire $X_0(p^n)$ attachée au groupe $\Gamma_0(p^n)$ n'ait qu'un nombre fini de K-points dès que $n \geqslant n_0$. En particulier, si E est une courbe elliptique définie sur K, la composante p-primaire du sous-groupe de torsion de E(K) est d'ordre borné par un nombre qui ne dépend que de p et de K.

(Le lien entre (M_7) et les courbes modulaires est moins fortuit qu'on ne pourrait penser : G. Bely a en effet prouvé que toute courbe algébrique sur $\bar{\mathbf{Q}}$ est « modulaire », i.e. peut être définie par un sous-groupe d'indice fini de $\mathbf{SL}_2(\mathbf{Z})$.)

Le théorème de Mumford

Ce théorème ne dit pas que C(K) est fini, mais seulement qu'il est « très rare ». De façon plus précise, supposons C plongée dans un espace projectif $\mathbf{P}_n$, et notons $N_{K,C}(X)$ le nombre des points $x \in C(K)$ tels que $H(x) \leqslant X$. Mumford démontre :

$$(M) \qquad N_{K,C}(X) \leqslant \lambda_r \log\log X + \mu,$$

où λ_r ne dépend que du rang r de $\Gamma = J(K)$ (on peut prendre $\lambda_r = 3 \cdot 5^r$, par exemple), et μ dépend de C, de K et du prolongement de C dans $\mathbf{P}_n$.

On a en particulier :

$$N_{K,C}(X) = O(\log \log X) \quad \text{pour } X \to \infty.$$

La croissance de la fonction $N_{K,C}(X)$ est donc plus lente que dans le cas $g = 1$ (où elle est de l'ordre d'une puissance de $\log X$) et bien plus lente que dans le cas $g = 0$ (où elle est de l'ordre d'une puissance de X).

La démonstration de Mumford repose sur une remarquable inégalité liant les hauteurs de deux points de C. Pour l'énoncer, il est commode de supposer que le diviseur D servant à plonger C dans J a été choisi tel que $(2g - 2)D$ appartienne à la classe canonique de C. Soit alors $\theta \in \mathrm{Pic}(J)$ la classe du « diviseur thêta » de la jacobienne J, et posons :

$$x.y = \hat{h}_\theta(x + y) - \hat{h}_\theta(x) - \hat{h}_\theta(y) \quad \text{si } x, y \in J(\overline{\mathbf{Q}}).$$

Mumford démontre que l'on a :

$$(M') \qquad x.y \leqslant \frac{1}{2g}(x.x + y.y) + \nu(C)$$

pour $x, y \in C(\overline{\mathbf{Q}})$ et $x \neq y$, où $\nu(C)$ est une constante ne dépendant que de la courbe C.

Le passage de (M') à (M) se fait par un argument élémentaire de géométrie des nombres.

J.-P. S.

Publications

J.-P. Serre, *Groupes algébriques associés aux modules de Hodge-Tate* (*Astérisque* n° 65, *Soc. Math. France*, 1979, p. 155-188).

— *Arithmetical Groups* (rédigé avec la collaboration de A. Robinson et C. Maclachlan, *Homological Group Theory*, édit. par C.T.C. Wall, *LMS Lect. Note Series* n° 36, Cambridge Univ. Press, 1979, p. 105-136).

— *Un exemple de série de Poincaré non rationnelle* (*Proc. Neder. Acad. Sci.*, t. 82, 1979, p. 469-471).

— *Quelques propriétés des groupes algébriques commutatifs* (*Astérisque* n° 69-70, *Soc. Math. France*, 1979, p. 191-202).

Édition

H. Cartan, *Œuvres* (3 vol., édit. par R. Remmert et J.-P. Serre, Springer-Verlag, 1979, 1498 p.).

F.A. Bogomolov, *Sur l'algébricité des représentations l-adiques* (*C. R. Acad. Sci. Paris,* série A, 290, 1980, p. 701-703).

Missions

Cours :

— *Selected Topics in Algebraic Geometry and Number Theory,* Harvard, septembre-décembre 1979.

Exposés :

— *Applications of Čebotarev's theorem to modular forms,* Durham, juillet 1979 ;

— *Galois representations and Hodge-Tate modules,* Inst. Adv. Study, Princeton, septembre 1979 ; Harvard, octobre 1979 ;

— *Varieties over finite fields, from Weil to Deligne,* Penn. State University, College Park, octobre 1979 ;

— *Points rationnels et points entiers sur les variétés algébriques,* Marseille, janvier 1980 ;

— *Rational points on algebraic varieties ;* Londres, février 1980 ; Stockholm, mars 1980 ;

— *Extensions icosaédrales,* Bordeaux, mars 1980 ;

— *Modular forms of one variable,* Stockholm, mars 1980 ;

— *Le grand crible - Application aux points rationnels des variétés algébriques,* Grenoble, avril 1980.