CAHIERS DU SÉMINAIRE D'HISTOIRE DES MATHÉMATIQUES

MARC HINDRY

Géométrie arithmétique

Cahiers du séminaire d'histoire des mathématiques 2^e série, tome 3 (1993), p. 79-84

<http://www.numdam.org/item?id=CSHM_1993_2_3__79_0>

GEOMETRIE ARITHMETIQUE

Marc HINDRY

"Le chercheur se laissera conduire dans ce domaine si attrayant par les remarquables analogies que l'on observe entre la théorie des fonctions algébriques d'une variable et celle des nombres algébriques. L'analogue du développement en série de puissances d'une fonction algébrique dans la théorie des nombres a été établi par Hensel; quant à l'analogue du théorème de Riemann-Roch, il a été traité par Landsberg [*Math. Annalen*, t. L , 1898] [...] Nous voyons que les trois branches fondamentales des mathématiques, à savoir la théorie des nombres, l'algèbre et la théorie des fonctions sont dans le rapport le plus intime [...]" (Hilbert, 12^{e} problème).

Ce thème est repris notamment par A. Weil dont une bonne partie de l'œuvre est émaillée de préoccupations sur l'analogie entre corps de fonctions et corps de nombres. Il n'est évidemment pas le seul; il cite souvent Artin, Hasse et glorifie en particulier le point de vue de Kronecker comme plus profond et supérieur à celui réputé plus élégant de Dedekind : "Dans son Grundzüge, Kronecker ne cherche pas seulement à donner son propre traitement des problèmes fondamentaux de la théorie des idéaux, qui forment le sujet principal des travaux de Dedekind; son but est plus haut. Il cherchait à décrire et initier une nouvelle branche des mathématiques qui contiendrait la théorie des nombres et la géométrie algébrique comme cas particuliers". Weil suggère qu'il s'agit d'un texte trilingue, les trois colonnes étant l'arithmétique, la géométrie algébrique et la géométrie de Riemann (analytique complexe). On peut considérer que le programme d'unification des deux premières est rempli par la théorie des schémas de Grothendieck et que les récents développements de la géométrie "à la Arakelov" constituent un volet de l'unification des trois thèmes. Je voudrais présenter quelques aspects élémentaires de ces idées et, à travers deux ou trois auteurs, l'évolution, les quelques succès de la théorie qu'on appelle aujourd'hui géométrie arithmétique.

Une idée mathématique aussi vaste (et vague parfois...) que l'unité de l'arithmétique et de la géométrie ne peut se mesurer seulement à ses "résultats" (les théorèmes qu'elle permet de démontrer), mais il est peut-être éclairant d'illustrer l'évolution de la théorie des équations diophantiennes sous cet angle .

Commençons par l'équation de Diophante : $x^2+y^2 = z^2$. Du point de vue arithmétique on trouve les solutions premières entre elles en notant que z est impair, x et y de parités opposées et $y^2 = (z+x)(z-x)$ entraîne $z-x = u^2$, $z+x = v^2$ et $y = uv$, et donc $x = (v^2-u^2)/2$ et $z = (v^2+u^2)/2$. Du point de vue géométrique on retrouve ces solutions en coupant la conique par la droite $u(z-x) + vy = 0$. On peut traiter dans ce style les courbes de genre 0. Faisant suite au mémoire de Poincaré paru en 1901 au

Journal de Liouville, Mordell traite en 1922 les courbes de genre 1 (du type $zy^2 = x^3+axz^2+bz^3$); celles-ci sont munies d'une addition définie géométriquement par "cordes et tangentes". Mordell prouve que les solutions forment un groupe de type fini (un nombre fini de solutions engendrent les autres) en utilisant notamment une notion de hauteur (*cf.* plus loin) et des arguments de descente analogues à ceux de Fermat ; il suggère aussi que le nombre de solutions devrait être fini quand le genre est au moins deux. Un des plus grand succès de la géométrie arithmétique est la démonstration de cette conjecture par Faltings en 1983 ; l'analogue sur les corps de fonctions avait été prouvé par Manin en 1963. Les idées (mais pas directement les résultats) d'Arakelov sont cruciales dans la preuve de Faltings, ainsi que la théorie des schémas de Grothendieck. Une nouvelle preuve a été donnée par Vojta en 1990 en "traduisant" dans le langage d'Arakelov une preuve qu'il avait lui-même élaborée sur les corps de fonctions.

1. Analogies entre $\mathbb{Z}$ et $\mathbb{C}[X]$

Ces deux anneaux sont factoriels, c'est-à-dire qu'il existe des éléments premiers (les nombres premiers ; les polynômes irréductibles unitaires) tel que tout élément a non nul s'écrive de manière unique :

$$a = \varepsilon P_1^{m_1}...P_r^{m_r}$$

où les P sont premiers et ε est un élément inversible (égal à +1 ou -1 ; égal à un nombre complexe non nul). Je noterai :

$$\mathrm{ord}_{P_i}(a) = m_i.$$

L'ensemble des places (ou valeur absolue à équivalence près) peut être décrit ainsi :
Sur $\mathbb{Z}$, on a $|a|_\infty$ = valeur absolue usuelle et $|a|_p = p^{-\mathrm{ord}_p(a)}$ et, lorsque v décrit l'ensemble de ces places, on a facilement la formule du produit :

$$\Pi |a|_v = 1.$$

Sur $\mathbb{C}[X]$, on a les places définies par $\log|a|_p = -\mathrm{ord}_p(a)$ et $\log|a|_\infty$ = degré de a ; on vérifie encore plus facilement la formule du produit (qui peut aussi s'interpréter comme le théorème des résidus d'après ce qui suit).
L'analogie est frappante, mais il y a aussi une différence cruciale : le comportement de $|a|_\infty$ est distinct des autres places de $\mathbb{Z}$; par exemple on n'a pas en général $|a+b|_\infty \leq \max(|a|_\infty, |b|_\infty)$; on dira que ∞ est une place archimédienne. Mais ceci ne se produit pas sur $\mathbb{C}[X]$; toutes les places jouent le même rôle comme l'interprétation géométrique suivante le fait voir : on considère $a \in \mathbb{C}[X]$ comme une fonction sur la sphère de Riemann $S=\mathbb{C} \cup \{\infty\}$ appelée aussi droite projective; on voit alors qu'à chaque premier P de $\mathbb{C}[X]$ correspond un nombre complexe α tel que $P = X-\alpha$ et $\mathrm{ord}_p(a)$ est l'ordre de la fonction au point $\alpha \in S$ alors que le degré de a n'est autre que l'ordre de la fonction au point $\infty \in S$.

Ces considérations sur les places peuvent être étendues aux anneaux des fonctions régulières sur une courbe affine (le rôle de S étant alors joué par la courbe projective associée) et aux anneaux d'entiers de corps de nombres, il y a alors plusieurs places à l'infini ou archimédiennes, disons r_1 places réelles et r_2 places complexes.

2. Théorèmes de Riemann-Roch et de Minkovski (selon Weil)

Dans le premier on compte la dimension d'un espace de fonctions, dans le second on compte le nombre de points dans une boîte.

Soit C une courbe algébrique (lisse, projective), un diviseur est une somme formelle de points (de places) à coefficients entiers : $D = \Sigma\, n_P\, P$. On dit que D est positif si ses coefficients le sont et on pose : $\deg(D) = \Sigma\, n_P$. Appelons K le corps des fonctions rationnelles sur C ; pour $f \in K$, on définit son diviseur : $\mathrm{div}(f) = \Sigma\, \mathrm{ord}_P(f)\, P$. Le théorème de Riemann-Roch sur C calcule la dimension l(D) de l'espace vectoriel $L(D) := \{f \in K \,/\, D+\mathrm{div}(f) \geq 0\}$.

Théorème de Riemann-Roch : il existe un entier $g \geq 0$ (le genre de la courbe C) tel que, si $\deg(D) \geq 2g+1$ alors $l(D) = \deg(D)-g+1$.

Par analogie, on définit un diviseur sur l'anneau A des entiers d'un corps de nombres K comme une somme formelle $D = \Sigma n_P\, P$ où P parcourt l'ensemble des places de K (on autorise des coefficients réels aux places archimédiennes) ; on pose :

$$\deg(D) = \Sigma\, n_P \log NP + \Sigma\, n_V$$

où la première somme est sur les places correspondant à un idéal premier P de norme NP = cardinal(A/P) et la deuxième sur les places archimédiennes. Pour x élément de K, on pose :

$$\mathrm{div}(x) = \Sigma\, \mathrm{ord}_P(x)\, P - \Sigma \log |x|_V.$$

On définit aussi $L(D) = \{x \in K/\ D + \mathrm{div}(x) \geq 0\}$, c'est un ensemble fini et un théorème de Minkovski (comptant le nombre de points d'un idéal dans une boîte $|x|_V \leq \exp(n_V)$) est équivalent à :

$$l(D) := \log(\mathrm{card} L(D)) = \deg(D) - g + \log w + \mathrm{reste}$$

où le terme "reste" tend vers zéro quand deg(D) tend vers l'infini, w = nombre des racines de l'unité dans K et $g = \log(2^{-r_1}(2\pi)^{-r_2}\sqrt{\Delta}\, w)$ où Δ désigne le discriminant de K.

On a donc l'analogue du genre ; la formule de Hurwitz se traduit bien :

Si $C' \to C$ est un revêtement de degré d non ramifié de courbes, alors

$$g' - 1 = d(g-1)$$

tandis que, pour une extension de degré d non ramifiée de corps de nombres, on a

$$g' - \log w' = d(g - \log w).$$

En fait on peut étendre ce parallèle aux extensions "modérément" ramifiées.

3. Théorie des hauteurs

Pour les problèmes diophantiens on est amené à introduire une notion de taille d'un point de l'espace projectif. Si $P = (x_0,...,x_n) \in \mathbb{P}^n(\mathbb{Q})$ avec les x_i entiers premiers entre eux, on pose :

$$H(P) := \max |x_i| \text{ et } h(P) := \log\max |x_i| .$$

On peut étendre la formule en posant :

$$h(P) := \Sigma \log\max |x_i|_v$$

où la somme est prise sur toute les places, lorsque P désigne un point dont les coordonnées x_i sont dans un corps de fonctions d'une courbe ou un corps de nombres. La formule du produit garantit que le résultat ne dépend pas des coordonnées choisies.
La notion de hauteur est essentielle pour la descente infinie et sur les corps de fonctions elle a une interprétation très géométrique :
Une variété X (par exemple $X = \mathbb{P}^n$) définie sur $K = k(C)$ (le corps des fonctions sur C) peut être vue comme une famille de variétés sur C, $p : X \to C$, et un point $P \in X(K)$ comme une section $s_P : C \to X$. On a alors $h(P) = \deg s_P^*(D)$ où D est une section hyperplane (un hyperplan si $X = \mathbb{P}^n$).
Curieusement ce point semble avoir échappé à Weil ; c'est Néron qui voit cela et de plus réalise le passage capital de cette interprétation géométrique aux corps de nombres . Le langage de Néron ne s'emploie guère de nos jours car à peu près à la même époque Grothendieck développe son langage des schémas qui constitue un pas de géant vers l'unification de la géométrie et de l'arithmétique. Je vais essayer de décrire les hauteurs "à la Néron" dans ce langage ce qui nous amène ensuite à la théorie d'Arakelov.

4. Le langage des schémas de Grothendieck et la géométrie d'Arakelov

Le langage des schémas permet enfin de parler de variété algébrique sur $\mathbb{Z}$ ou de considérer une courbe algébrique (sur un corps) et l'anneau des entiers d'un corps de nombres comme un "même" objet : un schéma de dimension un ; il confirme une intuition de Kronecker qui attribue la dimension n au corps $\mathbb{F}_p(X_1, ..., X_n)$ et n+1 au corps $\mathbb{Q}(X_1, ..., X_n)$.
Le schéma (affine) spec(A) a pour ensemble sous-jacent l'ensemble des idéaux premiers d'un anneau A muni de la topologie dite de Zariski : les fermés sont de la forme V(I) = {P premier/ I inclus dans P} où I est un idéal. Les idéaux premiers de $\mathbb{C}[X]$ correspondent aux points $a \in \mathbb{C}$ ou au point générique l'idéal {0}; les idéaux de $\mathbb{Z}$ aux places non archimédiennes (les nombres premiers) et au point générique {0}; en général les points "usuels" correspondent aux idéaux maximaux. Il faut aussi définir $\mathcal{O}$ un faisceau d'anneaux ; par exemple, sur l'ouvert $\text{spec}(\mathbb{Z}) \setminus V(n\mathbb{Z})$, on pose $\mathcal{O}(U) = \mathbb{Z}[1/n]$ et, si U est un ouvert d'une courbe on pose $\mathcal{O}(U)$ = anneau des fonctions rationnelles régulières sur U.
Si l'on a une variété algébrique X sur $\mathbb{Q}$, on peut en écrire des équations sur $\mathbb{Z}$ et lui

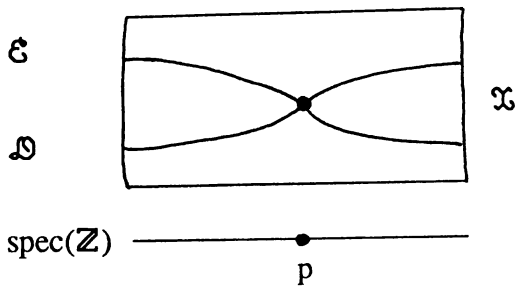
associer ainsi un schéma sur $\mathbb{Z}$: $\mathfrak{X} \to \text{spec}(\mathbb{Z})$ (si X est affine on choisit des équations $P_1(x_1, ..., x_n) = ... = P_r(x_1, ..., x_n) = 0$ avec des coefficients entiers et on pose $\mathfrak{X} = \text{spec}(\mathbb{Z}[x_1, ..., x_n]/(P_1, ..., P_r))$. Un point rationnel P correspond alors à une section $s_P : \text{spec}(\mathbb{Z}) \to \mathfrak{X}$. Si $\mathfrak{D}$ est un diviseur sur $\mathfrak{X}$ prolongeant un diviseur D section hyperplane, alors $s_P^*\mathfrak{D} = \Sigma\, n_p\, p$ est un diviseur sur spec($\mathbb{Z}$) et on est tenté, par analogie avec le cas géométrique, de poser $h(P) = \deg(s_P^*\mathfrak{D}) = \Sigma\, n_p \log p$, mais on voit bien qu'il manque la contribution des places à l'infini. La solution de Néron est de construire une fonction $G : X(\mathbb{C}) - \text{support}(D) \to \mathbb{R}$ telle que

$$h(P) = \deg(s_P^*\mathfrak{D}) + G(P) = \Sigma\, n_p \log p + G(P).$$

Ces idées ont été developpées par l'école russe : Shafarevic, Parshin et plus spécialement Arakelov. Ce dernier a poussé encore plus loin les analogies, jusqu'à obtenir en particulier un théorème de Riemann-Roch, une formule d'adjonction. Formellement on complète spec($\mathbb{Z}$) en lui ajoutant un point à l'infini et on complète $\mathfrak{X}$ en lui ajoutant une fibre au dessus de ∞ qu'on définit par $\mathfrak{X}_\infty = X(\mathbb{C})$ et qui est sensée représenter la partie géométrie complexe "à la Riemann", alors que $\mathfrak{X}$ est sensée décrire l'arithmétique ; par exemple, la fibre $\mathfrak{X}_p$ au dessus de p est la variété obtenue en réduisant mod p les équations de X. Quand $\mathfrak{X}$ est de dimension 2 (*i.e.* X est une courbe) Arakelov définit l'intersection de deux diviseurs sur $\mathfrak{X}$: pour deux sections $\mathfrak{D}$, $\mathfrak{E}$ correspondant à des points rationnels P et Q de $X(\mathbb{Q})$, elle est donnée par :

$$(\mathfrak{D},\mathfrak{E}) = \Sigma\, \text{mult}_p(\mathfrak{D},\mathfrak{E}) \log p + G(P,Q)$$

où mult_p est la multiplicité d'intersection au dessus de p, c'est-à-dire la plus grande puissance de p pour laquelle P et Q sont congrus et où G est une fonction de Green (une sorte de potentiel).



La hauteur s'interprète alors comme une intersection et l'on peut copier toutes les démonstrations géométriques utilisant les intersections. Toutefois il manque une notion de dérivation ou d'espace tangent sur spec($\mathbb{Z}$).

Cette géométrie qu'on appelle maintenant géométrie d'Arakelov est developpée notamment par Parshin, Szpiro, Moret-Bailly, Gillet et Soulé, Faltings.

Bibliographie succincte des textes utilisés

A. Weil, Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques (1939) 236-240 (*Œuvres*, Springer).
A. Weil, Lettre à Simone Weil (1940), 244-256 (*Œuvres*, Springer).
A. Weil, Number theory and algebraic geometry, *Proc. inter. Math. congress*, Cambridge Mass., vol.2, 90-100.

A. Néron, Arithmétique et classes de diviseurs sur les variétés algébriques, *Proc. Inter. Symp. on Algebraic Number Theory*, Tokyo, Nikko, 1955.
A. Néron, Quasi-fonctions et hauteurs sur les variétés abéliennes, *Ann. of math.*,.82 (1965), 249-331.

A. Grothendieck, *Eléments de Géométrie algébrique*, Publ. I.H.E.S., 1962.

S. Arakelov, Intersection theory of divisors on an arithmetic surface, *Izv. Akad. Nauk. SSSR*, sér. Math 38 (1974); *AMS translation*, 8 (1974), 1167-1180.
S. Arakelov,6 Theory of intersections on the arithmetic surface, *Proc. int. Congress Math.*, Vancouver (1974), 405-408.

Séminaire Bourbaki, exposés récents:
- Szpiro n°619 (1983);
- Soulé n°713 (1989);
- Szpiro n°729 (1990);
- Bost n°731 (1990).

L. Szpiro : séminaires relatifs à la conjecture de Mordell sur les corps de fonctions et sur les corps de nombres:
- Sur les pinceaux de courbes de genre au moins deux, *Astérisque*, 86 (1981)
- Sur les pinceaux arithmétiques, *Astérisque*, 127 (1985).

Dept. Math.
Université Paris 7
2 place Jussieu
75251 PARIS cedex