# MATHÉMATIQUES

## Principe local-global en arithmétique

David Harari[1]

### Introduction

Considérons un système d'équations

$$f_i(x_1, ..., x_n) = 0 \qquad i = 1, ..., r \tag{1}$$

où les $f_i$ sont des polynômes à coefficients dans $\mathbf{Z}$. Décider si ce système possède une solution en nombres entiers est une question en général très difficile. Les travaux de Davis, Putnam, Robinson et Matjasevic dans les années soixante ont du reste montré que ce problème était essentiellement indécidable [2].

Au lieu de considérer les solutions en nombres entiers, on peut s'intéresser aux solutions à valeurs dans le corps $\mathbf{Q}$ des rationnels. Si les polynômes $f_i$ sont homogènes, on ne considère que les solutions non triviales (i.e. différentes de $(0, ..., 0)$), et la question de l'existence d'une telle solution sur $\mathbf{Q}$ ou sur $\mathbf{Z}$ est bien sûr la même.

On peut aussi reformuler ces questions en termes géométriques. Dans le cas d'une famille de polynômes $f_i$ quelconques, il s'agit de déterminer si la *variété algébrique affine* définie par le système (1) possède un point entier, ou encore un point rationnel. Dans le cas d'une famille de polynômes homogènes, ces polynômes définissent une *variété algébrique projective*, et on se demande si cette variété possède un point rationnel.

Faute d'une méthode générale pour résoudre ces questions, il est naturel de chercher des conditions nécessaires, et la première idée consiste à utiliser des congruences. Voici un exemple classique, dû à Fermat :

**Proposition.** — *Soit $m$ un entier de la forme $m = 4^r(8s + 7)$ avec $r$ et $s$ entiers $> 0$. Alors l'équation*

$$x^2 + y^2 + z^2 = m$$

*n'a pas de solutions rationnelles.*

---

[1] Université Paris-Sud Orsay

[2] Pour une formulation plus précise de ce résultat, on pourra par exemple se reporter à [20].

*Démonstration.* S'il y avait une solution rationnelle, il y aurait une solution entière non triviale (en chassant les dénominateurs) pour l'équation

$$(8s+7)t^2 = x^2 + y^2 + z^2$$

Quitte à diviser $x, y, z, t$ par un même nombre, on peut alors supposer qu'ils sont premiers entre eux dans leur ensemble. On regarde ensuite l'équation modulo 4 : dans $\mathbf{Z}/4\mathbf{Z}$, les carrés sont 0 et 1 ; ainsi $t$ ne peut être pair sinon $x^2+y^2+z^2$ serait divisible par 4 ce qui impliquerait que $x, y, z$ soient tous pairs, en contradiction avec l'hypothèse. Mais si $t$ est impair, alors $(8s+7)t^2$ est congru à $-1$ modulo 8 et $x^2+y^2+z^2$ aussi, ce qui est impossible car les carrés de $\mathbf{Z}/8\mathbf{Z}$ sont $0, 1, 4$. $\square$

La méthode précédente peut se généraliser : pour trouver une condition nécessaire d'existence d'une solution rationnelle d'un système d'équations polynomiales, on se ramène à une équation en nombres entiers, et on essaie ensuite d'utiliser des congruences modulo $\mathbf{Z}/p^j\mathbf{Z}$ pour un certain nombre premier $p$ (ou plusieurs) et des entiers positifs $j$. Pour formuler plus commodément ces conditions, on a recours aux *corps p-adiques*; c'est ce qui donne naissance aux *conditions locales* qui font l'objet du paragraphe suivant.

## Les conditions locales

Le langage des corps $p$-adiques a été inventé par Hensel à la fin du XIX[e] siècle. Soit $p$ un nombre premier. On définit l'*anneau des entiers p-adiques* $\mathbf{Z}_p$ comme le complété de l'anneau $\mathbf{Z}$ pour la topologie associée à la valeur absolue $p$-adique : $| x |_p = p^{-v_p(x)}$, où $v_p(x)$ est la *valuation p-adique* de $x$, c'est-à-dire l'entier naturel $r$ tel que $p^r$ divise $x$ et $p^{r+1}$ ne divise pas $x$ (par convention $v_p(0) = +\infty$). Plus explicitement, l'anneau $\mathbf{Z}_p$ est la *limite projective* sur les entiers $n \geqslant 1$ des $\mathbf{Z}/p^n\mathbf{Z}$ (un élément de $\mathbf{Z}_p$ est donc une suite $(x_n)$ avec $x_n \in \mathbf{Z}/p^n\mathbf{Z}$, telle que l'image de $x_{n+1}$ par la surjection canonique $\mathbf{Z}/p^{n+1}\mathbf{Z} \to Z/p^n\mathbf{Z}$ soit $x_n$, ceci pour tout $n$). Le *corps p-adique* $\mathbf{Q}_p$ est le corps des fractions de $\mathbf{Z}_p$, ou encore le complété de $\mathbf{Q}$ pour la valeur absolue $| \,.\, |_p$. Pour plus de détails sur les propriétés des corps $p$-adiques, on pourra se référer à [27] ou [4]. Ces corps sont appelés des corps *locaux*, tout comme le corps des réels $\mathbf{R}$ qui est le complété de $\mathbf{Q}$ pour la valeur absolue usuelle. Par opposition, le corps $\mathbf{Q}$ est appelé un corps *global*. On pose par commodité $\mathbf{Q}_\infty = \mathbf{R}$, et on note $\mathcal{P}$ l'ensemble de tous les nombres premiers.

Il est alors équivalent de dire qu'un système d'équations polynomiales a une solution dans $\mathbf{Z}_p$ ou qu'il a une solution dans $\mathbf{Z}/p^j\mathbf{Z}$ pour tout entier $j \geqslant 1$. De même les conditions nécessaires de congruence pour avoir une solution rationnelle correspondent à l'existence de solutions (ou de solutions non triviales si on travaille avec des polynômes homogènes) dans $\mathbf{Q}_p$. Pour résumer :

**Proposition.** — *Une condition nécessaire (mais pas toujours suffisante) pour qu'un système d'équations polynomiales (resp. polynomiales homogènes) à coefficients dans* $\mathbf{Q}$ *ait une solution (resp. une solution non triviale) rationnelle est qu'il ait une solution (resp. une solution non triviale) dans tous les* $\mathbf{Q}_p$, *pour* $p \in \mathcal{P} \cup \{\infty\}$.

Ces *conditions locales* sont plus agréables à manipuler que les conditions de congruence modulo $\mathbf{Z}/p^j\mathbf{Z}$ car d'une part on n'a pour chaque $p$ qu'un corps $p$-adique à considérer, d'autre part travailler sur un corps est plus commode qu'avoir à calculer dans des anneaux qui ne sont pas intègres. En outre, décider si les conditions locales sont vérifiées pour un système donné est un processus *fini*. En effet le très important résultat suivant permet souvent de réduire la question de l'existence d'une solution dans $\mathbf{Q}_p$ à une solution dans $\mathbf{Z}/p\mathbf{Z}$ :

**Théorème (Lemme de Hensel).** — *Soit*

$$f_i(x_1, ..., x_n) = 0 \qquad 1 \leqslant i \leqslant r$$

*un système d'équations polynomiales à coefficients dans* $\mathbf{Z}$ *(ou même* $\mathbf{Z}_p$*). Alors si la réduction modulo p de ce système* [3] *possède une solution* **non singulière** *dans* $\mathbf{Z}/p\mathbf{Z}$*, le système possède une solution dans* $\mathbf{Z}_p$*.*

Ici, solution non singulière (ou *lisse*) signifie que la matrice des dérivées partielles $(\frac{\partial f_i}{\partial x_j})$ est de rang maximal (i.e. de rang $\inf(r, n)$) en cette solution ; s'il n'y a qu'une équation, ceci correspond au fait qu'au moins une dérivée partielle ne s'annule pas. En langage géométrique, le lemme de Hensel signifie : si la réduction modulo $p$ d'une $\mathbf{Z}_p$-variété possède un point lisse sur $\mathbf{Z}/p\mathbf{Z}$, alors la variété possède un $\mathbf{Z}_p$-point (qui est forcément lisse). Voici un exemple classique d'application du lemme de Hensel :

**Proposition.** — *Soient $p$ un nombre premier distinct de 2 et $a, b, c$ trois entiers relatifs non divisibles par $p$. Alors l'équation $ax^2 + by^2 = c$ possède une solution dans* $\mathbf{Z}_p$*.*

*Démonstration.* La réduction modulo $p$ de cette équation s'écrit $\bar{a}x^2 + \bar{b}y^2 = \bar{c}$, avec $\bar{a}$, $\bar{b}$, $\bar{c}$ non nuls dans $\mathbf{Z}/p\mathbf{Z}$. Mais cette dernière équation admet une solution dans $\mathbf{Z}/p\mathbf{Z}$ (pour le voir, on peut par exemple compter le nombre de carrés dans $\mathbf{Z}/p\mathbf{Z}$ : il y en a $\frac{p+1}{2}$, donc au moins un élément de $\mathbf{Z}/p\mathbf{Z}$ est à la fois de la forme $\bar{a}x^2$ et $\bar{c} - \bar{b}y^2$). Une telle solution est nécessairement non singulière, car le seul point où les deux dérivées partielles s'annulent est $(0, 0)$, qui n'est pas solution. On applique alors le lemme de Hensel. □

Le lemme de Hensel se démontre par le même algorithme que celui de la méthode de Newton pour les équations réelles (voir [27], II.2.2 pour une preuve détaillée). Il possède des raffinements qui permettent de toujours ramener la question de l'existence d'une $\mathbf{Q}_p$-solution à un processus fini. D'autre part, pour un système d'équations à coefficients entiers « raisonnable » [4], l'existence de points non singuliers modulo $p$ est automatique pour presque tout $p$. Ainsi, vérifier les conditions locales est en pratique facile. Par exemple pour une équation quadratique $ax^2 + by^2 = c$ comme ci-dessus, seuls les $p$ qui divisent $2abc$ sont à considérer d'après la proposition . D'autre part la condition « à l'infini » d'existence de solutions réelles est satisfaite si et seulement si $a$,$b$, et $-c$ ne sont pas tous du même signe.

Mentionnons enfin que tout ce qui précède se généralise aisément au cas d'un corps de nombres quelconques $k$ (c'est-à-dire d'une extension finie du corps $\mathbf{Q}$, par exemple $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-1})$...). On fait intervenir les complétés du corps $k$ pour

[3] Noter que comme $\mathbf{Z}_p/p\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$, la réduction modulo $p$ d'un entier $p$-adique dans $\mathbf{Z}/p\mathbf{Z}$ a un sens.

[4] « Raisonnable » correspond au fait que la variété algébrique associée soit *géométriquement intègre* ; les estimées de Lang-Weil donnent alors que pour $p$ assez grand, l'existence d'un point modulo $p$ est garantie.

ses diverses valeurs absolues ; un nombre fini d'entre elles sont *archimédiennes* (correspondant aux plongements réels et complexes de $k$), les autres sont *non archimédiennes* (ou *finies*), correspondant aux valuations définies par les idéaux premiers de l'anneau des entiers de $k$. Les « conditions locales » signifient qu'on a l'existence de solutions dans chaque complété $k_v$ de $k$, et le lemme de Hensel marche de manière analogue. Pour un corps de nombres $k$, on a ainsi à considérer l'ensemble de toutes ses *places*, i.e. l'ensemble de ses valeurs absolues modulo équivalence des distances qu'elles définissent.

La question est bien sûr maintenant de savoir s'il y a des cas où les conditions locales d'existence d'une solution sont suffisantes pour avoir une solution « globale » (à valeurs dans le corps de nombres sur lequel on travaille). Nous allons voir des exemples et contre-exemples au paragraphe suivant.

## Du local au global

L'un des premiers résultats (et peut-être le plus célèbre) de passage du local au global est le théorème suivant, démontré dans toute sa généralité par Hasse en 1924 (pour une preuve complète sur $\mathbf{Q}$, on pourra consulter [27], IV.3) :

**Théorème (Hasse-Minkowski).** — *Soit $q(x_1, ..., x_n)$ une forme quadratique sur un corps de nombres $k$. Alors elle possède un zéro non trivial si et seulement si elle possède un zéro non trivial dans tous les complétés de $k$.*

En langage géométrique, le théorème signifie qu'une quadrique projective sur un corps de nombres $k$ qui a des points dans tous les complétés de $k$ possède un point rationnel [5] (c'est-à-dire un point défini sur $k$). Le cas $n = 3$ est dû à Legendre. Le point le plus difficile consiste à passer du cas $n = 3$ au cas $n = 4$, le cas $n \geqslant 5$ résultant ensuite d'un argument de fibration (que nous retrouverons plus tard dans un contexte plus général). On constate d'ailleurs que les problèmes de passage du local au global en arithmétique sont souvent d'autant plus difficiles que le nombre de variables est petit. Du reste, si $n \geqslant 5$, l'existence de points locaux aux places finies est automatique pour une quadrique en $n$ variables ; du coup il suffit dans ce cas pour avoir l'existence d'un point rationnel de vérifier l'existence d'un point aux complétés réels de $k$, ce qui est très facile.

Un autre exemple connu de Hasse où le principe local-global vaut est celui de certaines équations *normiques*. Plus précisément soit $K/k$ une extension *cyclique* (i.e. galoisienne de groupe de Galois cyclique) de corps de nombres, fixons une base $(\omega_1, ..., \omega_r)$ du $k$-espace vectoriel $K$. On peut alors considérer l'équation :

$$N_{K/k}(x_1\omega_1 + ... + x_r\omega_r) = a \tag{2}$$

où $a$ est une constante de $k^*$, et les $x_1, ..., x_r$ sont les variables ; ici $N_{K/k}(.)$ est la norme de $K$ à $k$, c'est-à-dire l'application qui à un élément $x$ de $K$ associe le déterminant de la multiplication par $x$ dans le $k$-espace vectoriel $K$.

[5] Attention ici à la terminologie (classique mais quelque peu trompeuse) : point rationnel ne saurait signifier point défini sur $\mathbf{Q}$ puisque la quadrique elle-même n'est définie que sur une extension $k$ de $\mathbf{Q}$.

**Théorème (Hasse, 1924).** — *Pour une extension cyclique $K/k$, l'équation (2) possède une solution dans $k$ si et seulement si elle en possède une dans tous les complétés de $k$.*

Autrement dit un élément qui est une norme partout localement est une norme globale. Ce résultat est une conséquence de la théorie du corps de classes global (cf. [4], VII).

Par analogie avec les résultats précédents, on dira qu'une classe de variétés algébriques [6] lisses (i.e. sans point singulier) satisfait le *principe de Hasse* si pour toute variété dans cette classe, les conditions locales (existence d'un point dans tous les complétés de $k$) impliquent l'existence d'un point rationnel. Par exemple on a vu que les quadriques projectives satisfaisaient le principe de Hasse.

Rappelons que deux variétés $X$ et $Y$ sont $k$-birationnelles si elles possèdent respectivement des ouverts denses (pour la topologie de Zariski) $U$ et $V$, avec $U$ isomorphe (au-dessus de $k$) à $V$. Par exemple l'espace affine $\mathbf{A}^n_k$ et l'espace projectif $\mathbf{P}^n_k$ sont $k$-birationnels, une quadrique possédant un point rationnel est $k$-birationnelle à l'espace projectif (on dit qu'elle est $k$-rationnelle). Deux variétés sont $k$-birationnelles si et seulement si leurs *corps de fonctions* sont isomorphes (cf. [17], I.4).Si on travaille avec des variétés projectives et lisses sur $k$, alors le principe de Hasse est un *invariant $k$-birationnel* (s'il vaut pour une variété, il vaut pour toutes les variétés qui lui sont $k$-birationnelles), c'est donc une propriété dépendant seulement du corps des fonctions de la variété. Ce fait résulte de deux points importants : le théorème des fonctions implicites $p$-adique (qui dit que si une variété $X$ possède un point lisse dans un complété $k_v$ de $k$, tout ouvert Zariski-dense de $X$ possède aussi un tel point), et le lemme de Lang-Nishimura qui dit que l'existence d'un $k$-point est un invariant $k$-birationnel des variétés projectives et lisses (ceci sur tout corps $k$).

Ceci étant, on peut se demander s'il existe des contre-exemples au principe de Hasse (pour des variétés lisses). C'est effectivement le cas, comme Hasse lui-même l'avait remarqué, pour des équations normiques analogues à (2), quand l'extension $K/k$ n'est pas cyclique, mais par exemple galoisienne de groupe de Galois $(\mathbf{Z}/2\mathbf{Z})^2$. Avec $k = \mathbf{Q}$ et $K = \mathbf{Q}(\sqrt{13}, \sqrt{17})$, on obtient que $-1$ est une norme partout localement, mais n'est pas une norme globale (cf. [4], exercice 5.3). Plus tard, des contre-exemples furent trouvés pour des courbes de genre 1 (indépendamment par Reichardt et Lind vers 1940), puis par Swinnerton-Dyer pour les surfaces projectives lisses cubiques (1962). Ce dernier résultat est déjà plus surprenant car sur $\bar{k}$, une surface cubique lisse est birationnelle à l'espace projectif ; pourtant, il existe même des contre-exemples pour des surfaces cubiques « diagonales », comme celui-ci (dû à Cassels et Guy en 1966) :

$$5x^3 + 9y^3 + 10z^2 + 12t^3 = 0$$

Ces contre-exemples peuvent souvent s'expliquer par des lois de réciprocité venant de la théorie des nombres, par exemple la loi de réciprocité quadratique

6 Implicitement dans cet article, nous supposerons les variétés *géométriquement intègres* ; cette propriété signifie grosso modo que quand on regarde la variété sur la clôture algébrique $\bar{k}$, elle ne se décompose pas en union d'un nombre fini de variétés plus petites.

(cf. [27], I.3) ou ses généralisations, comme la suite exacte suivante, valable pour une extension cyclique (disons de degré $n$) $K/k$ de corps de nombres :

$$1 \to k^*/NK^* \to \bigoplus_v k_v^*/NK_v^* \to \mathbf{Z}/n\mathbf{Z} \to 1 \tag{3}$$

où la somme directe est prise sur tous les complétés $k_v$ de $k$, $N$ désigne la norme de $K$ à $k$, ou de $K_v = K \otimes_k k_v$ à $k_v$, et la flèche de droite est une application de réciprocité donnée par la théorie du corps de classes local. Cette suite exacte (qui vient du corps de classes global) donne un peu plus que le résultat de Hasse sur les équations normiques : pour une extension cyclique, un élément est une norme globale si et seulement s'il est une norme locale en toutes les places à l'exception possible d'une.

Indiquons comment une telle loi de réciprocité peut être utilisée pour montrer qu'une variété est un contre-exemple au principe de Hasse, en considérant l'exemple suivant dû à Iskovskih (1970) :

$$y^2 + z^2 = (3 - x^2)(x^2 - 2) \tag{4}$$

On se limite à l'ouvert lisse $U$ de cette $\mathbf{Q}$-variété défini par $y^2 + z^2 \neq 0$. Posons $K = \mathbf{Q}(\sqrt{-1})$. Une étude locale facile montre que $U$ a des points dans tous les complétés de $\mathbf{Q}$. Mais en utilisant le fait que $y^2 + z^2$ est une norme de l'extension $K/k$, on voit que si on pose $f(x) = (x^2 - 2)$, alors pour tout $\mathbf{Q}_p$-point $M_p$ de $U$ avec $p \neq 2$ (incluant $p = \infty$), on a $f(M_p)$ norme de l'extension $K_p/\mathbf{Q}_p$, où $K_p = K \otimes_{\mathbf{Q}} \mathbf{Q}_p$. Par contre pour $p = 2$, on obtient que $f(M_p)$ ne peut pas être une norme de $K_p/\mathbf{Q}_p$. Par conséquent, il ne peut y avoir de point rationnel $M$ dans $U$, sinon la classe du rationnel $f(M)$ dans $\mathbf{Q}^*/NK^*$ contredirait la suite exacte (3).

Il est logique d'essayer de trouver un cadre général permettant d'expliquer tous ces contre-exemples. Une approche particulièrement fructueuse a été introduite par Manin en 1970, dans son exposé au Congrès international. Elle consiste à faire intervenir le *groupe de Brauer* de la variété.

## Groupe de Brauer et principe de Hasse

Soit $X$ une variété algébrique lisse sur un corps $k$. Son groupe de Brauer (cohomologique) $\operatorname{Br} X$ est défini par le biais de la cohomologie étale de la variété $X$ (cf. [21], IV) : il s'agit du deuxième groupe de cohomologie étale à valeurs dans le faisceau $\mathbf{G}_m$. Pour ceux qui ne sont pas familiarisés avec la cohomologie étale, il nous suffira dans cet exposé de connaître les propriétés suivantes du groupe de Brauer :

– Pour une variété réduite à un point sur un corps $k$, le groupe de Brauer s'identifie à $\operatorname{Br} k$, groupe de Brauer du corps $k$ qu'on peut définir classiquement comme les classes d'équivalence d'algèbres simples centrales sur $k$ ([26], X.4 et X.5) munies du produit tensoriel. En particulier $\operatorname{Br} k = 0$ si $k$ est un corps fini ou un corps algébriquement clos.

– Si $X$ est une variété lisse, le groupe $\operatorname{Br} X$ est un sous-groupe du groupe de Brauer $\operatorname{Br}(k(X))$ du corps des fonctions $k(X)$ de $X$ (il correspond aux éléments *non ramifiés*, voir [7]).

– Le groupe de Brauer définit un foncteur contravariant des $k$-variétés vers les groupes abéliens. En particulier si une $k$-variété $X$ possède un point dans une extension $K$ de $k$, on a une application d'évaluation [7] en ce point : $\mathrm{Br}\,X \to \mathrm{Br}\,K$. On peut notamment appliquer ceci quand $k$ est un corps de nombres et $K = k$ ou $K$ est un complété $k_v$ de $k$.

– Pour un corps de nombres $k$ et l'un de ses complétés $k_v$, on dispose d'un homomorphisme injectif $j_v : \mathrm{Br}\,k_v \to \mathbf{Q}/\mathbf{Z}$ (l'*invariant local*) qui est un isomorphisme pour $v$ finie. Pour une place réelle $v$ on a $\mathrm{Br}\,k_v = \mathbf{Z}/2\mathbf{Z}$ et pour une place complexe $\mathrm{Br}\,k_v = 0$. On a également la loi de réciprocité globale donnée par la suite exacte (dont (3) est un cas particulier)

$$0 \to \mathrm{Br}\,k \to \bigoplus_v \mathrm{Br}\,k_v \xrightarrow{\sum j_v} \mathbf{Q}/\mathbf{Z} \to 0 \tag{5}$$

Notons d'ailleurs que l'injectivité dans cette suite exacte correspond au fait que les *variétés de Severi-Brauer* vérifient le principe de Hasse. Une variété de Severi-Brauer de dimension $n-1$ sur un corps $k$ est une variété qui devient isomorphe à l'espace projectif sur la clôture algébrique $\bar{k}$ de $k$. À une telle variété $X$ est associé un élément de $n$-torsion de $\mathrm{Br}\,k$ ([26], X.6), qui est nul si et seulement si $X$ possède un $k$-point. Le cas $n = 2$ correspond aux coniques.

L'idée de Manin est la suivante : soit $X$ une $k$-variété projective et lisse possédant un point rationnel $M$, on note $M_v$ le $k_v$-point de $X$ correspondant à $M$. Soit $\alpha \in \mathrm{Br}\,X$. Alors la famille des évaluations $(\alpha(M_v)) \in \bigoplus_v \mathrm{Br}\,k_v$ (la somme directe[8] étant prise sur tous les complétés de $k$) provient de $\mathrm{Br}\,k$ (par fonctorialité) puisque $(M_v)$ provenait d'un même point rationnel $M$. On a donc, d'après (5) :

$$\sum_v j_v(\alpha(M_v)) = 0 \tag{6}$$

Si une famille de points locaux $(M_v)$ satisfait cette condition pour tout $\alpha \in \mathrm{Br}\,X$, on dit qu'elle satisfait les *conditions de Manin*. A contrario, cela signifie que si pour toute famille de points locaux $(M_v)_{v\in\Omega}$ (où $\Omega$ désigne l'ensemble de toutes les places du corps de nombres $k$), il existe un $\alpha \in \mathrm{Br}\,X$ tel que $\sum_v j_v(\alpha(M_v)) \neq 0$, alors $X$ **ne peut pas avoir de point rationnel**. C'est ce qu'on appelle l'*obstruction de Manin* (ou de Brauer-Manin) au principe de Hasse.

Notons que le contre-exemple d'Iskovskih (4) rentre dans cette catégorie. Dans ce cas l'élément $\alpha$ de $\mathrm{Br}\,X$ utilisé est le *symbole de Hilbert* $(a, f(x))$ (dans le groupe $\mathrm{Br}\,(k(X))$ il correspond à l'algèbre de quaternions engendrée par $(1, i, j, k)$ avec les relations $ij = -ij = k$, $jk = -kj = i$, $ki = -ik = j$, $i^2 = -1$, $j^2 = a$, $k^2 = f(x)$ ; c'est un cas particulier d'algèbre simple centrale, qui est d'ordre 2 dans le groupe de Brauer). Sur tout corps $K$ de caractéristique $\neq 2$, un symbole de Hilbert $(a, b)$ est nul si et seulement si $b$ est une norme de l'extension $K(\sqrt{a})/K$ (le symbole $(a, b)$ correspond, en termes de variété de Severi-Brauer, à la conique projective

[7] Dans le langage de la géométrie algébrique, un $K$-point correspond à un morphisme de schémas $\mathrm{Spec}\,K \to X$, d'où par contravariance une flèche $\mathrm{Br}\,X \to \mathrm{Br}\,K$, vu que le groupe de Brauer du schéma $\mathrm{Spec}\,K$ est $\mathrm{Br}\,K$.

[8] Il y a ici une subtilité : le fait que la variété soit projective implique que la somme est finie parce que le groupe de Brauer de l'anneau des entiers de $k_v$ est nul ; les spécialistes reconnaîtront un argument de bonne réduction.

$y^2 - az^2 - bt^2 = 0$). Ainsi la loi de réciprocité générale (5) s'identifie dans ce cas particulier à (3).

Dans son texte du Congrès international [19], Manin démontre l'important résultat suivant :

**Théorème (Manin, 1970).** — *Soit $X$ une courbe projective lisse de genre 1* [9] *sur un corps de nombres $k$. Supposons que le groupe de Tate-Shafarevitch de la jacobienne de $X$ soit fini. Alors si $X$ possède une famille de points locaux $(M_v)_{v\in\Omega}$ satisfaisant (6) pour tout $\alpha \in \mathrm{Br}\, X$, elle possède un point rationnel.*

Rappelons que la *jacobienne* d'une courbe $X$ de genre 1 est une courbe elliptique $E$, i.e. une courbe projective lisse donnée par une équation homogène du type $y^2 t = P(x, y, t)$ avec $P$ polynôme homogène de degré 3. Sur la clôture algébrique $\bar{k}$, $X$ et $E$ sont isomorphes (la différence étant que $X$ ne possède pas forcément de point rationnel). Le *groupe de Tate-Shafarevitch* d'une courbe elliptique $E$ correspond aux classes d'isomorphismes de courbes de genre 1 de jacobienne $E$ qui ont des points dans tous les complétés. On conjecture qu'il est toujours fini (ce problème est fortement relié à la conjecture de Birch et Swinnerton-Dyer, qui vaut un million de dollars...).

La preuve du théorème précédent repose essentiellement sur le théorème de dualité de Cassels-Tate pour la cohomologie galoisienne des courbes elliptiques ([3]). Par la suite, les contre-exemples classiques (vus au paragraphe précédent) au principe de Hasse ont tous pu être expliqués par l'obstruction de Manin. De ce fait, beaucoup de travaux depuis une trentaine d'années ont consisté non pas à démontrer que des classes de variétés vérifient le principe de Hasse (ce qui arrive finalement relativement rarement une fois sorti des cas très particuliers), mais plutôt que l'obstruction de Manin au principe de Hasse est la seule pour certains types de variétés (ce qui est bien plus fréquent).

## Cas où l'obstruction de Manin est la seule

Mentionnons d'abord une autre propriété qui est très liée au principe de Hasse : soit $X$ une variété algébrique lisse sur un corps de nombres $k$, possédant un point rationnel. On dit que $X$ vérifie l'*approximation faible* si pour tout ensemble fini $S$ de places de $k$ et toute famille de points locaux $(M_v)_{v\in S}$ (chaque $M_v$ étant un point de $X$ défini sur le complété $k_v$), on peut trouver un point rationnel $M$ de $X$ arbitrairement proche des $M_v$ pour $v \in S$ ; autrement dit l'ensemble $X(k)$ des points rationnels est dense dans l'ensemble $\prod_{v\in\Omega} X(k_v)$ pour la topologie produit des topologies $v$-adiques.[10] Par exemple l'espace affine ou projectif vérifie l'approximation faible (pour la droite affine, c'est un théorème classique en théorie de nombres), tandis qu'une courbe elliptique ne la vérifie jamais.

Tout comme pour le principe de Hasse, le groupe de Brauer permet de définir une obstruction (dite obstruction de Manin) à l'approximation faible, introduite par Colliot-Thélène et Sansuc dans les années 70 : une famille de point locaux

[9] ou plus généralement un espace principal homogène sous une variété abélienne de groupe de Tate-Shafarevitch fini

[10] Si on demande en plus des propriétés d'intégralité du point $M$ aux autres places de $k$, on obtient la notion d'*approximation forte*, que nous ne discuterons pas ici ; les deux notions coïncident pour une variété projective.

$(M_v)_{v\in\Omega}$ ne peut pas être dans l'adhérence de $X(k)$ si elle ne vérifie pas, pour tout élément $\alpha$ de $\mathrm{Br}\, X$, l'égalité (6), à cause de la loi de réciprocité (5). On dira que l'obstruction de Manin à l'approximation faible est la seule pour $X$ si l'ensemble $X(k)$ des points rationnels est dense dans l'ensemble des points de $\prod_{v\in\Omega} X(k_v)$ qui vérifient (6) pour tout $\alpha$ de $\mathrm{Br}\, X$. C'est par exemple le cas si $X$ est une courbe elliptique (ou plus généralement une variété abélienne) de groupe de Tate-Shafarevitch fini, et dont les points rationnels sont denses dans $X(k_v)$ pour toute place archimédienne[11] $v$ ([33]).

Il semble raisonnable de penser que l'obstruction de Manin au principe de Hasse et à l'approximation faible est la seule pour des variétés dont la géométrie est relativement « simple », plus précisément pour celles (dites rationnelles) qui deviennent birationnelles à l'espace projectif sur la clôture algébrique de $k$ (Colliot-Thélène et Sansuc ont notamment conjecturé ce résultat pour les surfaces rationnelles). Par exemple le cas des surfaces cubiques et des intersections de deux quadriques dans $\mathbf{P}^4_k$ ou $\mathbf{P}^5_k$ font partie des problèmes les plus difficiles et les plus fondamentaux du domaine. Notons aussi que pour une intersection complète (par exemple une hypersurface) lisse de dimension au moins 3, l'obstruction de Manin s'évanouit automatiquement ; il n'empêche que pour démontrer des résultats de principe de Hasse pour de telles variétés, on est parfois obligé de faire intervenir des variétés de dimension plus petite (notamment pour les méthodes de fibration, cf. plus bas) pour lesquelles l'obstruction de Manin va intervenir.

Voici quelques cas où l'on a établi que l'obstruction de Manin au principe de Hasse et à l'approximation faible est la seule (on pourra se réferer à [6] ou [22] pour d'autres exemples) :

– Surfaces de Châtelet (Colliot-Thélène, Sansuc, Swinnerton-Dyer, 1984-1987, [10]) ; elles sont données par des équations du type

$$y^2 - az^2 = P(x)$$

où $a$ est une constante non nulle et $P$ un polynôme de degré 4. Une application frappante de ce résultat est la description des rationnels qui peuvent s'écrire sous la forme $\alpha^2+\beta^2+\gamma^4$ avec $\alpha,\beta,\gamma$ rationnels. Le même article contient également beaucoup de résultats sur les intersections de deux quadriques dans l'espace projectif, notamment le fait que le principe de Hasse vaut pour les intersections lisses de deux quadriques dans $\mathbf{P}^n_k$ si $n \geqslant 8$.

– Surfaces fibrées en coniques de degré 4 (Colliot-Thélène, Sansuc, Salberger, Skorobogatov, [5]) ou 3 (Salberger et Skorobogatov [24]). [12]

– Espaces principaux homogènes des groupes algébriques linéaires connexes (Sansuc, 1981 [25]).

– Plus généralement, espaces homogènes des groupes algébriques linéaires semi-simples, à stabilisateurs connexes ou abéliens (Borovoi, [1], [2]).

[11] Cette condition sur les places archimédiennes vient de ce que l'évaluation $\alpha(M_v)$ pour $v$ archimédienne est la même pour tous les points $M_v$ qui sont dans la même composante connexe de $X(k_v)$ ; autrement dit les conditions de Manin ne disent pas grand chose aux places réelles, et rien du tout aux places complexes.

[12] Pour une surfaces fibrée en coniques, le nombre de fibres dégénérées (non géométriquement intègres) est $8-d$, où $d$ est le degré ; le problème est a priori d'autant plus difficile que $d$ est petit, mais dans le cas $d=3$, l'existence d'un point rationnel est automatique. Le travail de Salberger et Skorobogatov concerne donc l'approximation faible.

Il y a principalement deux méthodes pour établir ces énoncés (certains sont d'ailleurs obtenus en combinant les deux) :

– La *méthode des fibrations* consiste à écrire la variété $X$ à laquelle on s'intéresse comme fibrée au-dessus d'une base $B$ vérifiant l'approximation faible (par exemple l'espace projectif). Si les fibres vérifient le principe de Hasse (resp. l'approximation faible), on espère pouvoir montrer la même chose pour l'espace total $X$. Ceci marche bien quand toutes les fibres sont géométriquement intègres et la base $B$ est projective parce que grâce aux estimées de Lang-Weil, il existe dans cette situation un ensemble fini de places $S$ en dehors duquel presque toutes les fibres ont des points locaux. Les premières applications subtiles de cette méthode remontent à [10]. Une version plus compliquée de la méthode des fibrations consiste à supposer seulement que l'obstruction de Manin au principe de Hasse et à l'approximation faible est la seule pour les fibres, et à en déduire la propriété analogue pour $X$. Les hypothèses requises dans ce cadre sont plus délicates ; nous renvoyons le lecteur à [13] pour plus de détails.

– La *méthode de descente* consiste à utiliser l'absence d'obstruction de Manin pour ramener la question du principe de Hasse (ou de l'approximation faible) sur $X$ à des variétés auxiliaires (dites de descente) de dimension plus grande mais de géométrie plus simple. Les fondements théoriques de cette méthode, due à Colliot-Thélène et Sansuc ([9]) sont assez complexes. On en trouvera un bon exposé dans [30]. Elle a par exemple été appliquée avec succès aux surfaces de Châtelet [10] (les variétés auxiliaires étant ensuite traitées par fibration).

Je ne parlerai pas dans cet article de la méthode du cercle, qui permet également d'établir des résultats de principe de Hasse et d'approximation faible, avec en plus des estimations quantitatives. Son inconvénient est qu'elle nécessite en général que le nombre de variables soit grand par rapport au degré, elle est donc peu adaptée aux variétés de petite dimension. Citons quand même le bel article de Skinner ([28]), et celui de Heath-Brown et Skorobogatov en 2002 sur les équations normiques ([18]) qui est le premier à combiner méthode de la descente et méthode du cercle.

Mentionnons enfin un très important résultat de Swinnerton-Dyer (2001, [32]) : il a établi le principe de Hasse pour les surfaces cubiques diagonales sur $\mathbf{Q}$ (moyennant la finitude du groupe de Tate-Shafarevitch des courbes elliptiques) lorsqu'une condition « proche » de celle de Manin est vérifiée. Il en a déduit (par une méthode de fibration simple) le principe de Hasse pour toute hypersurface cubique diagonale de dimension $\geqslant 3$ (toujours sous l'hypothèse sur le groupe de Tate-Shafarevitch). La preuve de ce théorème (trop complexe pour être exposée ici) est basée sur une stratégie qui s'est révélée très fructueuse, introduite par Colliot-Thélène, Skorobogatov et Swinnerton-Dyer dans l'article [11] (paru en 1998). Elle a aussi été appliquée avec succès en 2005 à certaines surfaces de Kummer ([31]). Si on suppose en plus l'*hypothèse de Schinzel* (une généralisation du théorème de la progression arithmétique de Dirichlet), cette technique donne également des résultats pour des familles plus générales de courbes de genre 1 ([11]) ; tout récemment O. Wittenberg ([34]) a pu établir, sous les deux conjectures ci-dessus, le principe de Hasse pour toute intersection lisse de deux quadriques dans $\mathbf{P}^5_k$ (il a également obtenu des résultats partiels si on remplace $\mathbf{P}^5_k$ par $\mathbf{P}^4_k$). En comparant avec le résultat (inconditionnel) de Colliot-Thélène, Sansuc et Swinnerton-Dyer pour les intersections lisses de deux quadriques dans $\mathbf{P}_k^8$, on retrouve le fait que les problèmes de principe de Hasse sont d'autant plus difficiles que la dimension est petite.

## Au-delà de l'obstruction de Manin

Le titre de ce dernier paragraphe est emprunté à l'article fondateur [29]. Bien qu'il ne soit pas raisonnable de penser que l'obstruction de Manin au principe de Hasse soit la seule pour toute variété projective et lisse sur un corps de nombres, il a fallu attendre plus de 25 ans après l'article de Manin pour qu'un contre-exemple soit donné par Skorobogatov. Plus précisément, il a montré le

**Théorème (Skorobogatov, 1997).** — *Il existe une surface bielliptique $X$ sur $\mathbf{Q}$ telle que $X$ possède une famille de points locaux $(M_v)$ vérifiant les conditions de Manin, mais $X$ ne possède pas de point rationnel.*

Une *surface bielliptique* est le quotient du produit de deux courbes elliptiques par un groupe fini agissant sans point fixe (dans l'exemple de Skorobogatov, ce groupe est $\mathbf{Z}/2\mathbf{Z}$). La preuve du théorème repose encore sur la théorie de la descente : l'existence d'un point rationnel sur $X$ impliquerait qu'une certaine famille de variétés auxiliaires $(Y_i)$ (ce sont des espaces principaux homogènes sur $X$ sous le groupe $\mathbf{Z}/2\mathbf{Z}$) ait la propriété que l'une d'elles a un point rationnel. Le fait que l'une de ces variétés ait des points dans tous les complétés de $\mathbf{Q}$ permet de montrer que l'obstruction de Manin au principe de Hasse s'évanouit pour $X$. Mais d'un autre côté, les $(Y_i)$ qui ont des points partout localement sont des contre-exemples au principe de Hasse (venant de l'obstruction de Manin !). Ainsi, c'est une sorte de version « itérée » de l'obstruction de Manin qui est utilisée.

Quelque temps après, Skorobogatov et moi-même ([15]) avons développé une théorie de la descente utilisant des espaces principaux homogènes sur la variété considérée, sous des groupes non abéliens (alors que la théorie classique est étroitement reliée aux espaces principaux homogènes sous les tores ou les groupes finis abéliens). Cette théorie a conduit à des obstructions au principe de Hasse et à l'approximation faible formulées en termes de cohomologie galoisienne non-abélienne. Elle a permis de donner un cadre général pour le contre-exemple au principe de Hasse de Skorobogatov, et également pour les contre-exemples à l'approximation faible (basés sur le groupe fondamental géométrique) de [14]. Plus récemment, elle a aussi conduit ([16]) à la construction de contre-exemples à l'approximation faible non expliqués par le groupe de Brauer pour des surfaces d'Enriques (qui ne sont pourtant pas très loin des variétés rationnelles ; en particulier leur groupe fondamental géométrique est réduit à $\mathbf{Z}/2\mathbf{Z}$).

On ne connaît pas de contre-exemple inconditionnel au principe de Hasse qui ne soit pas expliqué par les obstructions ci-dessus. On pense qu'il en existe pour des hypersurfaces lisses de grand degré, mais on n'a pas pour l'instant de méthode pour attaquer ce problème. Une autre question ouverte consiste à déterminer si l'obstruction de Manin au principe de Hasse est la seule pour les courbes de genre $\geqslant 2$

(en supposant toujours la finitude du groupe de Tate-Shafarevitch de leur jacobienne). La question analogue en remplaçant « points rationnels » par « zéros-cycles de degré 1 » a une réponse positive [13] ([23], [8], ou encore [12] pour une preuve rapide). Dans une autre direction, on peut penser que les obstructions non-abéliennes permettront de construire des contre-exemples au principe de Hasse ou à l'approximation faible, non expliqués par les conditions de Manin, pour les espaces homogènes de groupes algébriques à stabilisateurs finis non-abéliens. Par exemple la propriété d'approximation faible pour le quotient $X = SL_n/G$, où $G$ est un groupe fini est reliée, comme l'a remarqué Colliot-Thélène, au problème de Galois inverse : si $X$ vérifie l'approximation faible en dehors d'un nombre fini de places du corps de nombres $k$, alors $G$ est groupe de Galois sur $k$. Ce serait en particulier le cas si l'obstruction de Manin à l'approximation faible était la seule pour $X$, mais ce dernier point ne me semble pas très vraisemblable si le groupe $G$ est quelconque (en particulier non résoluble).

*Remerciements.* Je tiens à remercier J.-L. Colliot-Thélène pour sa lecture attentive du manuscrit et ses pertinentes suggestions.

## Références

[1] M. V. Borovoi : Abelianization of the second nonabelian Galois cohomology, *Duke Math. J.* **72**, 217–239 (1993).

[2] M. V. Borovoi : The Brauer–Manin obstruction for homogeneous spaces with connected or abelian stabilizer, *J. reine angew. Math.* **473**, 181–194 (1996).

[3] J.W.S. Cassels : Arithmetic on curves of genus 1. VII. The dual exact sequence, *J. Reine Angew. Math.* **216**, 150–158 (1964).

[4] J.W.S. Cassels, A. Fröhlich : *Algebraic number theory*, Academic press, London and New-York, 1967.

[5] J.-L. Colliot-Thélène : Surfaces rationnelles fibrées en coniques de degré 4, in Séminaire de théorie des nombres de Paris 1988–1989, éd. C. Goldstein, Progress in Math. Birkhäuser **91**, 43–55 (1990).

[6] J.-L. Colliot-Thélène : L'arithmétique des variétés rationnelles (exposé fait à l'occasion de la remise du prix Fermat), *Annales de la Faculté des sciences de Toulouse*, vol. I,**3**, 295-336 (1992).

[7] J.-L. Colliot-Thélène : Birational invariants, purity and the Gersten conjecture, dans *K-theory and algebraic geometry : connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*, 1–64, *Proc. Sympos. Pure Math.* **58**, Part 1, Amer. Math. Soc., Providence, RI, 1995.

[8] J.-L. Colliot-Thélène : Conjectures de type local-global sur l'image des groupes de Chow dans la cohomologie étale, in *Algebraic K-theory* (Seattle, WA, 1997), Proc. Sympos. Pure Math. **67**, 1–12, Amer. Math. Soc., Providence, RI, 1999.

[9] J.-L. Colliot-Thélène, J.-J. Sansuc : La descente sur les variétés rationnelles II, *Duke Math. J.* **54**, 375–492 (1987).

[10] J.-L. Colliot-Thélène, J.-J. Sansuc, Sir Peter Swinnerton-Dyer : Intersection of two quadrics and Châtelet surfaces, *J. reine angew. Math.* **373** 37–107 ; **374**, 72–168 (1987).

[11] J.-L. Colliot-Thélène, A.N. Skorobogatov, Sir Peter Swinnerton-Dyer : Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, *Invent. Math.* **134**, no. 3, 579–650 (1998).

[12] D. Eriksson, V. Scharaschkin : On the Brauer-Manin obstruction for zero-cycles, prépublication 2005.

[13] D. Harari : Méthode des fibrations et obstruction de Manin, *Duke Math. J.* **75**, 221–260 (1994).

[13] Colliot-Thélène a conjecturé que ceci se généralisait à toute variété projective et lisse.

[14] D. Harari : Weak approximation and non-abelian fundamental groups, *Ann. Sci. École Norm. Sup.*, 4$^e$ série, **33**, 467–484 (2000).
[15] D. Harari, A.N. Skorobogatov : Non-abelian cohomology and rational points, *Comp. Math.* **130** 241–273 (2002).
[16] D. Harari, A.N. Skorobogatov : Non-abelian descent and the arithmetic of Enriques surfaces, *Int. Math. Res. Notices*, à paraître.
[17] R. Hartshorne : *Algebraic Geometry*, Springer-Verlag, New-York Heidelberg Berlin 1977.
[18] R. Heath-Brown, A.N. Skorobogatov : Rational solutions of certain equations involving norms, *Acta Math.* **189**, no. 2, 161–177 (2002).
[19] Yu. I. Manin : Le groupe de Brauer-Grothendieck en géométrie diophantienne, in *Actes du Congrès Intern. Math. (Nice 1970)*, Tome **1**, 401-411, Gauthiers-Villars, Paris 1971.
[20] Y. Matiyasevic : Diophantine representation of recursively enumerable predicates, in *Actes du Congrès Intern. Math.* (Nice, 1970), Tome 1, pp. 235–238. Gauthier-Villars, Paris, 1971.
[21] J. S. Milne : *Étale Cohomology*, Princeton Univ. Press, Princeton N.J. 1980.
[22] E. Peyre : Obstructions au principe de Hasse et à l'approximation faible, Séminaire Bourbaki, Vol. 2003/2004. Astérisque **299**, 2005.
[23] Shuji Saito : Some observations on motivic cohomology of arithmetic schemes, *Invent. Math.* **98**, 371–404 (1989).
[24] P. Salberger, A. N. Skorobogatov : Weak approximation for surfaces defined by two quadratic forms, *Duke Math. J.* **63**, 517–536 (1991).
[25] J.-J. Sansuc : Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, *J. reine angew. Math.* **327**, 12–80 (1981).
[26] J.-P. Serre : *Corps Locaux*, Hermann, Paris 1968.
[27] J.-P. Serre : *Cours d'arithmétique*, PUF, Paris 1970.
[28] C. Skinner : Forms over number fields and weak approximation, *Compositio Math.* **106**, no. 1, 11–29 (1997).
[29] A. N. Skorobogatov : Beyond the Manin obstruction, *Inv. Math.* **135**, 399–424 (1999).
[30] A. N. Skorobogatov : *Torsors and rational points*, Cambridge Univ. Press, 2001.
[31] A. N. Skorobogatov, Sir Peter Swinnerton-Dyer : 2-descent on elliptic curves and rational points on certain Kummer surfaces, à paraître dans *Adv. in Math.*
[32] Sir Peter Swinnerton-Dyer : The solubility of diagonal cubic surfaces, *Ann. Sci. École Norm. Sup.* (4) **34**, no. 6, 891–912 (2001).
[33] L. Wang : Brauer-Manin obstruction to weak approximation on abelian varieties, *Israel J. Math.* **94** (1996), 189–200.
[34] O. Wittenberg : Principe de Hasse pour les surfaces de Del Pezzo de degré 4, thèse de l'Université de Paris-Sud, 2005.

© Ivan Cori

*J.-C. Yoccoz lors de sa conférence du 13 avril 2005*
*à la Bibliothèque nationale de France*

# Une erreur féconde du mathématicien Henri Poincaré

Jean-Christophe Yoccoz

*Nous remercions Jean-Christophe Yoccoz de nous avoir autorisé à publier ce texte qui correspond à sa conférence donnée à la Bibliothèque nationale de France le 13 avril 2005 dans le cadre du cyle « Un texte, un mathématicien ». La* Gazette *105 avait présenté ce cycle de conférences organisé par la SMF et la BnF en partenariat avec France Culture et la revue* Tangente. *Le succès de ces manifestations a encouragé les organisateurs à renouveler l'expérience cette année, qui débutera le 11 janvier 2006 avec une conférence d'Yves Meyer*[1].

---

> *« ... For, in respect to the latter branch of the supposition, it should be considered that the most trifling variation in the facts of the two cases might give rise to the most important miscalculations, by diverting thoroughly the two courses of events, very much as, in arithmetic, an error which, in its own individuality, may be inappreciable, produces, at length, by dint of multiplication at all points of the process, a result enormously at variance with truth. ... »*
>
> *Edgar Allan Poe*
> *The mystery of Marie Roget, 1843*

> *« ... Car, relativement à la dernière partie de la supposition, on doit considérer que la plus légère variation dans les éléments des deux problèmes pourrait engendrer les plus graves erreurs de calcul, en faisant diverger absolument les deux courants d'événements ; à peu près de la même manière qu'en arithmétique une erreur qui, prise individuellement, peut être inappréciable, produit à la longue, par la force accumulative de la multiplication, un résultat effroyablement distant de la vérité ... »*
>
> *Trad. Charles Baudelaire, 1864*

La citation précédente est sans doute une des premières descriptions de ce qui a, beaucoup plus récemment, été baptisé d' « effet papillon », l'idée qu'à cause du caractère instable des évolutions dynamiques associées au système météorologique, le battement d'ailes d'un papillon pourrait sur le long terme être à l'origine de tempêtes et autres cataclysmes. Dans la bouche du chevalier Dupin, c'est à la logique d'une enquête policière plutôt qu'à la météorologie qu'est associée ce phénomène.

Le héros de notre histoire, Henri Poincaré (1854-1912) naît à Nancy, 11 ans après la parution de la nouvelle de Poe. Reçu premier à l'École polytechnique, il soutient en 1879 une thèse dont une des parties, le « *Mémoire sur les propriétés des fonctions définies par les équations différentielles* », annonce une des directions

[1] Tous les renseignements nécessaires se trouvent à l'adresse : `http://smf.emath.fr/BNF/2006/`

que prendront ses recherches. Après un bref passage à Caen, il est de retour à Paris dès 1881 et occupera à la Sorbonne à partir de 1886 une chaire de « Physique mathématique et Calcul des probabilités ».

Henri Poincaré est le plus grand mathématicien de son temps, l'un des 4 ou 5 plus importants de tous les temps. Son œuvre s'étend aussi à la physique. Avec Lorentz et Einstein, il est le codécouvreur de la théorie de la relativité restreinte. Par ailleurs, ses textes de philosophie des sciences exercent encore aujourd'hui une influence considérable. Son œuvre proprement mathématique est immense, de la géométrie à l'analyse et la topologie. Il est aussi le fondateur de la théorie des systèmes dynamiques ; c'est à cette partie de ses travaux que se rattache l'épisode qui nous intéresse ici.

Stockholm est certainement l'une des plus belles villes du monde, tout particulièrement au printemps où l'éclosion de la nature et la mer partout présente y créent une atmosphère exceptionnelle. À quelques kilomètres du centre, Djürsholm abrite au bord d'un bras de mer de splendides résidences, dont l'Institut Mittag-Leffler. Cet institut, avec la superbe bibliothèque autour duquel il s'organise, était il y a un siècle la demeure de Gösta Mittag-Leffler (1846-1927), le second personnage de notre histoire. C'est aujourd'hui l'un des hauts lieux de la recherche mathématique en Europe.

Mittag-Leffler fut un mathématicien de tout premier ordre, spécialiste d'analyse complexe, disputant avec le chimiste Alfred Nobel la première place dans le monde scientifique suédois de l'époque. Après un doctorat à Uppsala, il a voyagé à Paris, Berlin, Gottingen, collaborant avec Hermite, Weierstrass, Schering. Il a fondé au début des années 1880 la revue « *Acta Mathematica* », qui est toujours aujourd'hui l'une des trois ou quatre revues les plus prestigieuses en mathématiques au plan international.

Mittag-Leffler a su convaincre le roi Oscar de Suède et de Norvège (1829-1907) de soutenir financièrement la fondation d'Acta. Le roi, qui a été lui-même étudiant à Uppsala, est un mécène généreux pour l'activité scientifique. Mittag-Leffler propose donc au souverain de financer un prix qui célèbrerait son 60$^{e}$ anniversaire.

Le jury est constitué de Mittag-Leffler lui-même, de Charles Hermite (1822-1901) et de Karl Weierstrass (1815-1897). La prééminence de ces deux mathématiciens de la génération précédente au sein des écoles française et allemande garantit au prix une large audience.

L'annonce officielle est faite à la mi 1885 ; la date limite de soumission est fixée au 1$^{er}$ juin 1888. Le mémoire vainqueur sera publié dans les « *Acta mathematica* », et récompensé d'une médaille d'or accompagnée de 2 500 couronnes (le salaire annuel de Mittag-Leffler est de 7 000 couronnes). Les candidats peuvent traiter l'un des 4 sujets proposés, ou un sujet libre de leur choix. Sur les 12 mémoires reçus, 6 se prévalent de cette possibilité, tandis que 5 se rattachent au premier sujet proposé, le problème des $n$ corps en mécanique céleste.

Hermite a contribué à la fondation des « Acta Mathematica ». Poincaré a été étudiant de Hermite, il a publié un article dans chacun des 5 premiers volumes de la revue. Il connaît Mittag-Leffler et n'a pas fait mystère de sa volonté de participer au concours. Malgré l'anonymat des soumissions, Mittag-Leffler n'a pas grand mal à identifier son collègue français comme l'auteur d'un mémoire qui se détache très nettement du lot. Ce mémoire, intitulé « Sur le problème des trois corps et les équations de la dynamique » fait très rapidement l'unanimité du jury. Le résultat est proclamé le 20 janvier 1889. L'autre mémoire distingué par le jury est l'œuvre de Paul Appell et porte sur le développement en séries trigonométriques des fonctions abéliennes.

Le mémoire de Poincaré aurait dû être publié dans les « *Acta mathematica* » en octobre 1889. Il en sera autrement...

Lars Phragmen (1863-1937) est un jeune mathématicien suédois que Mittag-Leffler a chargé de la lecture détaillée des mémoires soumis. À la suite de ses commentaires, le mémoire de Poincaré, long de 160 pages initialement, s'est enrichi de 90 pages de notes supplémentaires. Vers juillet 1889, Mittag-Leffler transmet à Poincaré une demande d'éclaircissement de Phragmen. Poincaré s'aperçoit que les objections de Phragmen sont fondées, et découvre en reprenant le corps de son argumentation qu'il a commis une erreur sérieuse dans une autre partie du texte. Début décembre, il annonce à Mittag-Leffler que la rectification de l'erreur nécessite des changements substantiels dans son mémoire.

Craignant peut-être pour sa réputation scientifique, qui est moins établie que celle de Weierstrass, Hermite ou Poincaré lui-même, Mittag-Leffler récupère discrètement les quelques exemplaires du mémoire initial qu'il avait distribués à un cercle restreint de mathématiciens et astronomes. Il obtient de Poincaré que celui-ci règle les frais d'impression du mémoire initial, soit 3 500 couronnes, 1 000 de plus que le montant du prix. La version révisée, longue de 270 pages, est prête en avril 1890 et paraîtra dans les « *Acta mathematica* » en novembre 1890.

Voilà pour les circonstances historiques, pour lesquelles le livre de June Barrow-Green cité en référence[2] m'a été précieux. Venons-en au contenu scientifique de l'épisode : je vais essayer d'expliquer l'erreur de Poincaré, la découverte à laquelle la rectification de cette erreur l'a mené, et le retentissement de cette découverte sur les mathématiques d'aujourd'hui.

Il faut d'emblée affirmer que même si l'on retranche au mémoire tout ce qui touche à l'erreur et à sa révision, le contenu en reste extraordinairement riche. Poincaré lui-même en développera les idées dans les trois tomes des « *Méthodes Nouvelles de la Mécanique Céleste* », qui paraîtront entre 1892 et 1899, et marqueront une refondation complète du domaine. On trouve aussi, dans la première partie du mémoire, ce qu'on appelle aujourd'hui le théorème de récurrence de Poincaré ; ce résultat constitue l'acte fondateur de la théorie ergodique, branche cousine des systèmes dynamiques. Erreur ou pas, le prix était amplement mérité. Mais de tout ceci, je ne vais pas parler.

Un système dynamique, c'est un espace des phases avec une équation d'évolution ; les points de l'espace des phases décrivent les états possibles du système considéré ; l'équation d'évolution gouverne les changements d'états sur le court terme. Le but de la théorie est de comprendre l'évolution sur le long terme.

Souvent, un état peut-être déterminé par un nombre fini de paramètres et l'équation d'évolution est une équation différentielle décrivant la variation infinitésimale de ces paramètres. Poincaré, dès ses premiers travaux dans le domaine, va introduire un changement de point de vue fondamental. Ses prédécesseurs traitaient les équations différentielles comme des équations, et cherchaient à en

[2] Réf. : June Barrow-Green, *Poincare and the three-body problem (1997), AMS-LMS History of mathematics, Vol. 11.*

représenter les solutions par des formules toujours plus sophistiquées. Poincaré va s'apercevoir que, pour la plupart des équations différentielles, on ne peut disposer d'aucune formule raisonnable. Il va traiter les équations différentielles comme des objets géométriques, une révolution conceptuelle qui ouvre des perspectives complètement inédites. C'est dans cet esprit que j'ai complètement évité les formules dans ce qui suit.

La mécanique céleste traite du mouvement des corps célestes — étoiles, planètes, satellites naturels ou artificiels, astéroïdes...— sous l'action de la gravitation classique, à l'exclusion de tous autres phénomènes physiques. La loi de gravitation universelle de Newton stipule que la force d'attraction mutuelle de deux corps est proportionnelle à chacune de leurs masses, et inversement proportionnelle au carré de leur distance.

Dans le problème des $n$ corps, les corps célestes sont assimilés à des masses ponctuelles sans diamètre. L'état du système est donc déterminé par les trois coordonnées de position et les trois coordonnées de vitesse de chacun des corps : l'espace des phases est de dimension égale à $6n$ ; l'équation d'évolution est l'équation différentielle du second ordre qui traduit la loi de gravitation universelle.

Lorsqu'il y a seulement 2 corps, il n'est pas difficile de résoudre ces équations. Les solutions en ont en fait été découvertes par Kepler par l'observation céleste plus d'un siècle avant que Newton n'écrive ses équations. Chacun des corps parcourt une ellipse, le centre de masse occupant un des foyers de ces ellipses homothétiques ; l'aire parcourue par le rayon joignant le centre de masse à l'un des corps est balayée à vitesse constante (on peut avoir aussi une hyperbole ou une parabole au lieu d'une ellipse, mais les corps s'échappent alors à l'infini).

La situation considérée par Poincaré dans son mémoire est le problème restreint des trois corps, le cas le plus simple après celui de deux corps. Dans ce problème restreint, on fait les hypothèses suivantes. On suppose d'abord que l'un des corps, appelons-le $m$, est de masse nulle. Il n'influence donc en rien le mouvement des deux autres corps, appelons-les $m_1$ et $m_2$ , mais subit l'attraction gravitationnelle de ces corps. On suppose de plus que les corps $m_1$ et $m_2$, dont le mouvement doit obéir aux lois de Kepler, se déplacent à vitesse uniforme sur des cercles concentriques (dont le centre est le centre de gravité de ces deux corps). On cherche à comprendre la trajectoire du corps $m$, et on ne s'intéresse qu'aux trajectoires contenues dans le même plan que celles de $m_1$ et $m_2$. On suppose enfin que le rapport des masses de $m_2$ et $m_1$ est faible ; on note $\mu$ ce petit paramètre.

Pour déterminer l'état du système, il faut connaître les deux coordonnées de position et les deux coordonnées de vitesse du corps $m$ dans le plan où se déroule le mouvement. L'espace des phases est donc de dimension 4. Le plus simple est en fait de se placer dans un repère tournant qui accompagne la rotation uniforme des corps $m_1$ et $m_2$. Dans ce repère, ces deux corps deviennent immobiles, ce qui simplifie l'écriture des forces de gravitation, mais introduit un terme correspondant à la force de Coriolis. Néanmoins, le système d'équations différentielles obtenu a la forme générale, dite hamiltonienne, associée à la plupart des systèmes d'origine mécanique ; une conséquence fondamentale de cette propriété est la conservation au cours du temps d'une certaine fonction, le hamiltonien, calculable à partir de l'état du système. Cela veut dire que les solutions, qui sont des courbes dans l'espace des phases paramétrées par le temps, sont tracées sur les hypersurfaces (de dimension 3) représentant les différents niveaux possibles du hamiltonien (dans les situations classiques de la mécanique, le hamiltonien n'est rien d'autre que l'énergie totale du système).

Fixons le niveau du hamiltonien. Nous avons donc une hypersurface de dimension 3 sur laquelle sont tracées des courbes paramétrées par le temps. Dans cette hypersurface, Poincaré considère une surface $\Sigma$ (de dimension 2) transverse à la famille de courbes. Les équations d'évolution se traduisent par une transformation $T$ de cette surface $\Sigma$ dans elle-même : étant donné un point $x$ de $\Sigma$, on considère la courbe solution passant par $x$ à l'instant 0 et on désigne par $T(x)$ le premier point où cette courbe solution rencontre à nouveau $\Sigma$. Il s'agit donc à présent de comprendre les itérations successives de cette transformation $T$ de la surface $\Sigma$. On est passé d'une dynamique à temps continu en dimension 3 à une dynamique à temps discret en dimension 2.

Lorsque le paramètre $\mu$, rapport des masses de $m_2$ et $m_1$, est nul, il est facile d'analyser complètement la dynamique. Le corps $m_1$ est immobile à l'origine et le corps $m$, ne subissant pas l'attraction de $m_2$ décrit une ellipse (ou une hyperbole, ou une parabole ; mais c'est le cas de l'ellipse qui nous intéresse dans la suite) dont l'origine est un foyer. Dans le repère tournant, cette ellipse présente un mouvement de rotation apparent traduisant la rotation uniforme de $m_2$ autour de l'origine. Il y a donc superposition de deux mouvements périodiques : la rotation du grand axe de l'ellipse (dans le repère tournant) à une vitesse angulaire uniforme et le déplacement sur l'ellipse du corps $m$ en balayant les aires à vitesse uniforme (deuxième loi de Kepler). Les périodes des deux mouvements sont indépendantes et en général incommensurables : le mouvement dans son ensemble n'est alors pas périodique. On dit que le système est *complètement intégrable* et que la dynamique correspondante est *quasipériodique*.

Pour la dynamique de la transformation $T$ sur la surface $\Sigma$, cela se traduit de la façon suivante. La surface $\Sigma$ est feuilletée par un système de courbes fermées ; chacune de ces courbes est invariante par la transformation $T$ ; de plus, chacune de ces courbes peut être paramétrée par une coordonnée angulaire de façon que la transformation $T$ s'exprime comme une rotation dans cette coordonnée. L'angle de cette rotation dépend de la courbe considérée, et correspond au rapport des périodes des deux mouvements périodiques dans le cas du temps continu. Lorsque cet angle compté en nombre de tours, est un nombre rationnel, chaque point de la courbe est périodique sous l'action de $T$. Lorsqu'au contraire cet angle est irrationnel, et c'est le cas pour la plupart des courbes, les images successives d'un point de la courbe forment un ensemble dense dans la courbe.

Que se passe-t-il lorsque le paramètre $\mu$ n'est pas nul, mais simplement très petit ? Dans quelle mesure va-t-on retrouver certains des aspects du cas $\mu = 0$ ? Poincaré analyse d'abord le cas des orbites périodiques. Considérons pour fixer les idées le cas d'une courbe de $\Sigma$, invariante par $T$ lorsque $\mu = 0$, pour laquelle l'angle de la rotation induite par $T$ s'annule. Tous les points de cette courbe sont donc fixés par $T$ lorsque $\mu = 0$. Lorsque $\mu$ est petit mais non nul, Poincaré montre que seul un nombre fini de points (très voisins de cette courbe) sont encore fixés par $T$, et correspondent donc à des orbites périodiques pour le système en temps continu (dans le repère tournant).

Une analogie avec un système mécanique plus simple, le pendule, est utile. On considère le mouvement dans un plan vertical d'une barre rigide fixée à une de ses extrémités. En l'absence de pesanteur (correspondant au cas $\mu = 0$ pour le problème restreint des 3 corps), on a un mouvement de rotation uniforme ; en particulier toutes les positions sont des positions d'équilibre. Par contre, en présence de pesanteur, il n'y a plus que deux positions d'équilibre. La position verticale basse est un équilibre stable, la perturbation de cet équilibre conduit à de petites oscillations. La position verticale haute est un équilibre instable ; si, à un temps infiniment lointain dans le passé, la barre s'éloigne de cet équilibre avec une vitesse infiniment petite, elle effectuera un tour complet pour revenir à l'équilibre à un temps infiniment lointain dans le futur avec une vitesse infiniment faible. Ce comportement remarquable est qualifié de doublement asymptotique par Poincaré ; le vocabulaire moderne est homocline.

Revenons aux points fixés par la transformation $T$ sur la surface $\Sigma$. Poincaré montre que la moitié d'entre eux sont stables et l'autre moitié sont instables, au moins au niveau infinitésimal. Le passage de la stabilité infinitésimale à la stabilité locale ne sera obtenu que vers 1960 grâce aux succès de la théorie KAM (pour Kolmogoroff-Arnold-Moser) ; ce n'est pas ici notre sujet. Poincaré étudie de plus près les points fixes instables. Pour chacun de ces points fixes, Poincaré démontre qu'il existe une courbe remarquable tracée sur $\Sigma$ passant par ce point fixe, dite stable ou positivement asymptotique, caractérisée par la propriété suivante : quand on itère la transformation $T$ à partir d'un point de cette courbe, la suite de points obtenue ainsi converge vers le point fixe. Il existe de même une courbe, dite instable ou négativement asymptotique, caractérisée par la propriété duale : quand on itère l'inverse $T^{-1}$ de la transformation $T$ à partir d'un point de cette courbe, la suite de points obtenue ainsi converge vers le point fixe. Chacune de ces courbes est invariante sous l'action de la transformation $T$. Dans l'exemple du pendule pesant, les trajectoires homoclines associées à l'équilibre instable constituent à la fois la courbe stable et la courbe instable (il y a deux trajectoires homoclines suivant le sens de rotation du tour effectué).

Les courbes positivement et négativement asymptotiques des points fixes instables de la transformation $T$ coïncident-elles, comme c'est le cas pour le pendule pesant ? Dans le cas du pendule pesant, outre un calcul direct, un argument de portée plus générale est le suivant : on a affaire à une dynamique en temps continu dans un espace des phases bidimensionnel ; le théorème d'unicité des solutions d'équations différentielles garantit alors que les deux courbes asymptotiques sont égales dès qu'elles se rencontrent (en un point distinct du point fixe auquel elles sont associées).

Poincaré va chercher à déterminer la position de ces courbes positivement et négativement asymptotiques, en effectuant des développements par rapport aux puissances successives du petit paramètre $\mu$ (plus exactement, de la racine carrée de $\mu$). Dans la version initiale du mémoire, il montre que les deux courbes coïncident au premier ordre en $\sqrt{\mu}$ ; il affirme aussi que les développements en les puissances successives de $\sqrt{\mu}$ sont convergents. Dans la version corrigée du mémoire, il montre que les deux courbes coïncident à tous les ordres en $\sqrt{\mu}$ ; si les développements étaient effectivement convergents, cela permettrait évidemment de conclure que les deux courbes sont égales. Hélas, la convergence, qu'il pensait être conséquence de principes généraux valables dans des situations similaires, n'a pas lieu : lui-même le montrera dans la version corrigée !

On peut penser que Poincaré, en rédigeant la version initiale du mémoire, avait vérifié que les deux courbes coïncident à tous les ordres en $\sqrt{\mu}$ et donc (convaincu qu'il était alors de la convergence des développements) qu'elles étaient égales. Pour éviter le calcul délicat de ce développement à tous les ordres, il va chercher un raccourci en complétant le calcul (facile) au premier ordre en $\sqrt{\mu}$ par un argument de nature topologique. À la base de cet argument se trouve la propriété que $T$ préserve les aires, propriété héritée de la nature hamiltonienne du système initial. L'argument montre effectivement que les deux courbes doivent se rencontrer (en un point distinct du point fixe instable). En temps continu, pour le pendule pesant, cela implique que les deux courbes coïncident. Mais pas en temps discret, comme c'est le cas pour la transformation $T$ !

En résumé, les arguments, grâce auxquels Poincaré pensait initialement pouvoir conclure que les courbes positivement et négativement asymptotiques coïncident, permettent seulement de prouver que ces courbes se rencontrent en des points distincts des points fixes auxquels elles sont associées. En général, en ces points d'intersection, les droites tangentes aux deux courbes sont distinctes ; les trajectoires correspondantes sont dites homoclines transverses.

Quand on cherche, comme Poincaré lui-même l'a fait, à tracer dans toute leur extension des courbes positivement et négativement asymptotiques présentant des intersections homoclines transverses, on s'aperçoit rapidement que le fait que ces courbes soient invariantes par la transformation $T$ force une géométrie d'une complexité redoutable. Si Poincaré est bien conscient de cette complexité, il reviendra aux successeurs de Poincaré, George D. Birkhoff (1884-1944) et Steve Smale (né en 1930) de commencer à l'analyser.

Un des outils conceptuels fondamentaux, introduit par Alexandre Liapounov (1857-1918), est la mesure du taux de divergence (ou convergence) exponentielle des trajectoires au niveau infinitésimal. Pour le pendule pesant, cette divergence est toute entière concentrée au point d'équilibre instable. En présence de points d'intersections homoclines transverses, cette divergence exponentielle va se manifester pour toutes les trajectoires correspondant aux points d'intersection. C'est une telle divergence exponentielle qui caractérise les dynamiques de type chaotique qui sont à la base de l' « effet papillon ».

Le fer à cheval de Smale est un modèle simplifié de la transformation $T$ où l'on est capable de décrire complètement le système d'intersections homoclines transverses associé à un point fixe instable. Un codage géométrique simple permet d'associer à chaque point d'intersection des courbes positivement et négativement asymptotiques une suite de 0 et de 1 (paramétrée par les entiers relatifs, et ne comportant qu'un nombre fini de 1). Inversement, toute suite de 0 et de 1 ayant ces propriétés est associés à un point d'intersection. La suite associée à l'image $T(x)$ d'un point d'intersection $x$ est simplement la suite associée à $x$ décalée d'un cran vers la gauche. Quand on ne considère que la partie de la suite paramétrée par les entiers positifs ou nuls (cela revient à se concentrer sur l'évolution future en oubliant le passé), le passage de $x$ à $T(x)$ revient à multiplier par 2 le nombre dont la suite tronquée est le développement binaire : on retrouve la citation de Poe...

Malgré tous les progrès accomplis depuis une cinquantaine d'années dans notre analyse des systèmes dynamiques chaotiques (hyperboliques est le terme généralement utilisé par les mathématiciens), on aurait tort de croire que le problème restreint des 3 corps est aujourd'hui compris de façon satisfaisante. Une question centrale de la théorie des systèmes dynamiques, et qui est complètement ouverte à l'heure actuelle, est la suivante : choisissons au hasard un point de la surface $\Sigma$, et observons son orbite par les itérations successives de la transformation $T$. Y-a-t-il une probabilité non nulle (sur le choix du point initial) pour qu'on observe le long de cette orbite une divergence exponentielle des orbites au niveau infinitésimal ? La théorie KAM mentionnée auparavant nous garantit qu'à l'inverse il y a une probabilité non nulle de ne **pas** observer de divergence exponentielle car la dynamique de l'orbite sera de nature quasipériodique...

## Un texte, un mathématicien

Devant le succès rencontré l'an dernier, la SMF et la BnF ont décidé de poursuivre l'expérience. Un cycle de 4 conférences de mathématiques est organisé en 2006, elles s'adressent au grand public ainsi qu'aux enseignants des collèges-lycées, étudiants et lycéens.

C'est à la Bibliothèque nationale de France, les mercredis à 18h30, (site F. Mitterrand, Grand auditorium, Hall Est) Quai François-Mauriac, à Paris dans le 13e arr.

Date des conférences :

11 janvier Y. Meyer – *Pourquoi Henri Lebesgue essayait de mesurer les surfaces, et n'y arrivait pas ?*

15 mars É. Ghys – *Henri Poincaré et le monde non euclidien*

05 avril M. Audin – *Le cas de Sophie Kowaleskaya*

10 mai É. Bayer-Fluckiger – *Hermann Minkowski, grand prix de l'Académie des sciences à 18 ans*

Pour plus de détails voir la page web : `http://smf.emath.fr/BNF/2006/`