Points rationnels, zéro-cycles et lois de réciprocité

Jean-Louis Colliot-Thélène (CNRS et Université Paris-Sud)

Colloquium
Institut de mathématiques de Toulouse
Université Paul Sabatier, Toulouse (III)
29 novembre 2013

Voici un argument sous-jacent dans le Théétète de Platon.

L'équation $x^2 = 2$ n'a pas de solution dans $\mathbb{Q}$.

Démonstration.
Tout entier est soit pair $(2n)$ soit impair $(2n+1)$. Le produit d'un impair par un impair est impair.
Si l'on a une solution de $x^2 = 2$ dans $\mathbb{Q}$, alors on a des entiers $p > 0, q > 0$ avec $p^2 = 2q^2$. On prend q aussi petit que possible.
L'équation donne : p^2 est pair. Ceci force p à être pair, soit $p = 2p'$. Donc $4p'^2 = 2q^2$. Donc $2p'^2 = q^2$. Mais alors q^2 est pair, donc q est pair, soit $q = 2q'$. Mais alors $p'^2 = 2q'^2$ et $q' < q$, contradiction.

Autre exemple, plus récent mais pas beaucoup plus compliqué. Soit p un nombre premier. L'équation homogène

$$x^3 + py^3 + p^2z^3 = 0$$

n'a pas de solution en rationnels $(x, y, z) \neq (0, 0, 0)$.

Démonstration.
S'il y avait une solution, on pourrait la prendre avec x, y, z entiers sans facteur commun. De l'équation on déduit que p divise x^3, donc p divise x. Alors p^2 divise py^3 donc p divise y. Alors p^3 divise p^2z^3 donc p divise z. Contradiction.
L'argument montre qu'il n'y a pas de solution "primitive" de $x^3 + py^3 + p^2z^3 = 0$ dans l'anneau $\mathbb{Z}/p^3$.

Une condition nécessaire pour qu'une équation polynomiale $f(x_1, \ldots, x_n) = 0$ à coefficients entiers ait une solution en entiers est que la même équation ait des solutions dans tous les anneaux quotients $\mathbb{Z}/m$, ou encore dans tous les anneaux quotients $\mathbb{Z}/p^r$ pour tous les premiers p et toutes les puissances p^r.
Une autre condition nécessaire est l'existence de solution dans le corps $\mathbb{R}$ des réels.

Depuis Hensel (1897), nous savons comment reformuler les conditions de congruence.
Pour chaque premier p, on dispose de l'anneau des entiers p-adiques $\mathbb{Z}_p = \mathrm{limproj}_r \mathbb{Z}/p^r$, qui est *intègre*. On note son corps des fractions $\mathbb{Q}_p$.
Pour f un polynôme quelconque (resp. homogène) à coefficients entiers, la condition $f = 0$ a des solutions (resp. primitives) modulo tous les p^r pour $r > 0$ variable se traduit par : f a une solution (resp. primitive) dans $\mathbb{Z}_p$, et dans le cas homogène, c'est équivalent à dire : f a une solution non nulle dans le corps $\mathbb{Q}_p$.
On définit $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$.

Pour $X/\mathbb{Q}$ une variété algébrique sur $\mathbb{Q}$, c'est-à-dire un système d'équations polynomiales

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, m$$

à coefficients dans $\mathbb{Q}$, on a pour les points rationnels les inclusions

$$X(\mathbb{Q}) \hookrightarrow X(\mathbb{A}_{\mathbb{Q}}) \subset \prod_p X(\mathbb{Q}_p),$$

où $X(\mathbb{A}_{\mathbb{Q}})$ est l'ensemble des adèles de X (points entiers pour presque tout p).
Pour X "projectif" , c'est-à-dire donné par un système d'équations *homogènes* à coefficients dans $\mathbb{Q}$, pour lequel on considère les solutions différentes de $(0, \ldots, 0)$, on a $X(\mathbb{A}_{\mathbb{Q}}) = \prod_p X(\mathbb{Q}_p)$.

On dit que le principe local-gobal, ou le principe de Hasse, vaut pour une classe donnée d'équations si, pour $X/\mathbb{Q}$ dans cette classe, $\prod_p X(\mathbb{Q}_p) \neq \emptyset$ implique $X(\mathbb{Q}) \neq \emptyset$.
On dit que l'approximation faible vaut pour $X/\mathbb{Q}$ si $X(\mathbb{Q}) \subset \prod_p X(\mathbb{Q}_p)$ est dense dans le produit topologique.

Exemple historique (Legendre, Hilbert, Minkowski, Hasse) : la classe des quadriques, définies dans l'espace projectif $\mathbb{P}^n$, $n \geq 2$, par une forme quadratique non singulière $q(x_0, \ldots, x_n) = 0$ à coefficients dans $\mathbb{Q}$.

Coniques $q(x_0, x_1, x_2) = 0$ (Legendre, Paris, An VI (1797-1798); Gauß 1801; Hilbert 1899)

Si une conique a des points dans tous les $\mathbb{Q}_p$, elle a des points dans $\mathbb{Q}$.
Il suffit qu'elle ait des points dans tous les $\mathbb{Q}_p$ sauf peut-êre un.
Ceci est une conséquence de la *loi de réciprocité quadratique* et de ses compléments (Gauß). Plus généralement, on associe à toute conique $C/\mathbb{Q}$ et à tout premier p un invariant dans $\mathbb{Z}/2$, valant 0 si et seulement si la conique C a un point dans le corps $\mathbb{Q}_p$. *La somme de ces invariants vaut* 0 *dans* $\mathbb{Z}/2$.

Quadriques (Hasse, 1922-1924)

Soit $P(t) = \alpha t + \beta$, $\alpha, \beta \in \mathbb{Z}, \alpha.\beta \neq 0$.
Considérons l'équation affine

$$ax_0^2 + bx_1^2 = cx_2^2 + dx_3^2 = P(t) \neq 0$$

avec$a, b, c, d \in \mathbb{Z}$ non nuls.
Si on a des solutions dans tous les $\mathbb{Q}_p$, le théorème de Dirichlet sur les nombres premiers dans une progression arithmétique permet de trouver $t_0 \in \mathbb{Q}$ avec $P(t_0) \neq 0$ tel que $P(t_0)$ soit produit de puissances de premiers dans un ensemble S fini déterminé par les coefficients du système, contenant 2 et les premiers divisant l'un des a, b, c, d, et d'un unique nombre premier non contrôlé ℓ, et que le système donné ait des solutions dans tous les $\mathbb{Q}_p$ pour $p \in S$.

Le système

$$ax_0^2 + bx_1^2 = cx_2^2 + dx_3^2 = P(t_0)$$

a alors des solutions en les x_i dans tous les $\mathbb{Q}_p$ sauf peut-être dans $\mathbb{Q}_\ell$. Alors chacune des *coniques* $ax_0^2 + bx_1^2 = P(t_0)$ et $cx_2^2 + dx_3^2 = P(t_0)$ a des solutions dans $\mathbb{Q}$ d'après ce qu'on a vu plus haut. D'où solution de

$$ax_0^2 + bx_1^2 = cx_2^2 + dx_3^2 = P(t) \neq 0$$

Quadriques $q(x_0, x_1, x_{2,}x_3) = 0$
Si l'on part de $ax_0^2 + bx_1^2 = cx_2^2 + dx_3^2 \neq 0$, on définit un polynôme $P(t) = \alpha t + \beta$ par approximation à partir de solutions dans $\mathbb{Q}_p$ en les premiers de mauvaise réduction, et on procède comme ci-dessus.

Le principe local-global et l'approximation faible pour $q(x_0, \ldots, x_n) = 0$ et $n \geq 4$ se déduisent du cas de 4 variables par une méthode générale, montrant en particulier que le principe de Hasse vaut pour toute équation affine du type

$$\sum_{i=1}^{r} a_i x_i^2 = P(t) \neq 0$$

avec les $a_i \in \mathbb{Q}$ non nuls, $P(t) \in \mathbb{Q}[t]$ non nul de degré quelconque, et $r \geq 3$. [Mais pas $r = 2$].

On peut aussi facilement établir le principe de Hasse pour toute équation affine du type

$$\sum_{i=1}^{r} a_i(t)x_i^2 = P(t) \neq 0$$

avec les $a_i(t)$ et $P(t)$ polynômes non nuls dans $\mathbb{Q}[t]$ et $r \geq 4$. [Mais pas $r = 3$].

La **méthode du cercle** établit le principe local-global pour les hypersurfaces non singulières de degré d dans $\mathbb{P}^n_{\mathbb{Q}}$ quand n est "grand" par rapport à d.

Conjecture H (Bouniakowsky, Dickson, Schinzel 1958 ; Hardy et Littlewood)

Soient $P_i(t), i = 1, \ldots, m$ dans $\mathbb{Z}[t]$ des polynômes irréductibles de coefficient dominant positif, premiers entre eux deux à deux et tels qu'il n'y ait pas diviseur commun aux $\prod_i P_i(m)$ pour m variant dans $\mathbb{Z}$. Alors il existe une infinité d'entiers m tels que chacun des $P_i(m)$ est un nombre premier.

Exemple 1. Un polynôme $P(t) = t^2 + 1$
Exemple 2. $P_1 = t$, $P_2(t) = t + 2$. Nombres premiers jumeaux.

Observation (CT et Sansuc, 1979; développé 1991-1998 sur tout corps de nombres par Serre, Swinnerton-Dyer, CT, Skorobogatov)
En reprenant l'argument de Hasse, on montre :
"Théorème" **Sous l'hypothèse H**, *le principe de Hasse et l'approximation faible valent pour*

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

avec $a \in \mathbb{Q}^\times$ *et* $P(t) \in \mathbb{Q}[t]$ **irréductible**.

Plus généralement, sous H, le principe de Hasse et l'approximation faible valent pour

$$Norm_{K_i/\mathbb{Q}}(\Xi_i) = P_i(t), i = 1, \ldots, m$$

avec les extensions $K_i/\mathbb{Q}$ extensions *cycliques* de corps et les $P_i(t)$ dans $\mathbb{Q}[t]$ **irréductibles**, premiers entre deux à deux.

L'**astuce de Salberger** (1988), comme dégagée dans CT-Skorobogatov-Swinnerton-Dyer en 1998, est un substitut pour l'hypothèse H. Elle dit que quitte à faire des extensions de corps de $\mathbb{Q}$ convenables de degré assez grand, on a un énoncé de primalité.

Soient $P_i(t), i = 1, \ldots, m$ dans $\mathbb{Q}[t]$ des polynômes irréductibles de coefficient dominant positif, premiers entre eux deux à deux.
Il existe un ensemble fini S de premiers p dépendant uniquement des P_i tel que :
Pour tout entier $N \geq \sum_i \deg(P_i(t))$, il existe une extension de corps $k/\mathbb{Q}$ de degré N et, sur le corps k un élément $\theta \in K$ et des valuations w_i de k telles que chaque $P_i(\theta)$ satisfasse :
$w_i(P_i(\theta)) = 1$ et $w(P_i(\theta)) = 0$ pour w différent de w_i et non au-dessus d'un premier dans S.

C'est facile.
Traitons le cas des premiers jumeaux, $P_1(t) = t$ et $P_2(t) = t + 2$.
Ici on veut $N \geq 2$.
On choisit des premiers p et q quelconques. Soit $R(t) \in \mathbb{Z}[t]$ un polynôme unitaire de degré $N - 2$. Soit
$P(t) = R(t)t(t + 2) + qt + p(t + 2)$. Pour $R(t)$ et p, q assez généraux, c'est un polynôme irréductible. Soit $k = \mathbb{Q}[t]/P(t)$, et soit θ l'entier algébrique qui est la classe de t. On a clairement $\mathrm{Norm}_{k/\mathbb{Q}}(\theta) = \pm 2p$ et $\mathrm{Norm}_{k/\mathbb{Q}}(\theta + 2) = \pm 2q$.

La loi de réciprocité sur un corps de nombres k (Brauer, Hasse, Noether 1935) implique qu'une équation $\mathrm{Norm}_{K/k}(\Xi) = c$ avec $c \in k^\times$ et K/k extension cyclique satisfait le principe de Hasse, et même que cette équation a une solution dès qu'elle a une solution dans tous les complétés k_v de k en toute place sauf peut-être une. Remplaçant l'hypothèse H par l'astuce de Salberger, on montre inconditionnellement :

Théorème (cas particulier de Salberger 1988) *Si l'équation*

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

avec $a \in \mathbb{Q}^\times$ *et* $P(t) \in \mathbb{Q}[t]$ **irréductible** *a des solutions dans tous les* $\mathbb{Q}_p$*, alors l'indice de l'équation, c'est-à-dire le pgcd des degrés des extensions de corps* $K/\mathbb{Q}$ *sur lesquelles elle admet une solution, est égal à 1.*
On dit alors que la variété considérée possède un zéro-cycle de degré 1.

Revenons aux points rationnels. La conjecture H sur les polynômes à une variable est toujours ouverte. Mais les travaux de Green, Tao, puis Green, Tao et Ziegler on permis d'établir certaines versions à deux variables de cette conjecture pour les systèmes de formes linéaires.

Théorème (Green, Tao, Ziegler, 2010-2012)

Soient $L_i(x, y), i = 1, \ldots, r$ des formes linéaires à coefficients entiers non proportionnelles deux à deux, et soient $c_i \in \mathbb{Z}, i = 1, \ldots, r$. Supposons que pour tout premier p, il existe $(m, n) \in \mathbb{Z}^2$ tel que p ne divise aucun $L_i(m, n) + c_i$. Soit $K \subset \mathbb{R}^2$ un cône convexe ouvert contenant un point $(m, n) \in \mathbb{Z}^2$ avec chacun des $L_i(m, n) > 0$. Il existe une infinité de paires $(m, n) \in K \cap \mathbb{Z}^2$ tels que chaque $L_i(m, n) + c_i$ soit premier.

En combinant une conséquence élégante de ce résultat et les arguments évoqués ci-dessus (Hypothèse H + loi de réciprocité impliquent principe de Hasse), on obtient le résultat suivant.

Théorème (Harpaz, Skorobogatov, Wittenberg 2013)
Soient $K_i/\mathbb{Q}$, $i = 1, \ldots, r$ des extensions cycliques de $\mathbb{Q}$ et soient $e_i \in \mathbb{Q}$ et $b_i \in \mathbb{Q}^\times$ pour $i = 1, \ldots, r$. Alors le principe de Hasse et l'approximation faible valent pour les solutions rationnelles du système

$$\mathrm{Norm}_{K_i/\mathbb{Q}}(\Xi_i) = b_i(u - e_i v) \neq 0.$$

Le cas où les extensions $K_i/\mathbb{Q}$ sont quadratiques avait été obtenu antérieurement par Browning, Matthiesen et Skorobogatov (2012). Leur travail, première application des résultats de combinatoire additive à l'étude des points rationnels, repose sur les travaux de Green et Tao et un travail de Matthiesen.
De façon curieuse, l'argument de réciprocité, qui utilise la cyclicité des extensions $K_i/\mathbb{Q}$, n'intervient pas dans leur travail.

De fait, tout récemment, Browning et Matthiesen (2013) ont établi le résultat général suivant.

Théorème *Soient $K_i/\mathbb{Q}$, $i = 1, \ldots, r$ des extensions* **quelconques** *de corps de $\mathbb{Q}$ et soient $L_i(u_1, \ldots, u_s)$ avec $s \geq 2$ des formes linéaires à coefficients dans $\mathbb{Q}$, deux à deux non proportionnelles. Alors le principe de Hasse et l'approximation faible valent pour les solutions rationnelles du système*

$$\mathrm{Norm}_{K_i/\mathbb{Q}}(\Xi_i) = L_i(u_1, \ldots, u_s) \neq 0.$$

Rappelons que pour une extension quelconque $K/\mathbb{Q}$ de corps de nombres et $c \in \mathbb{Q}^\times$, le principe de Hasse ne vaut pas toujours pour une équation $Norm_{K/\mathbb{Q}}(\Xi) = c$. Il ne suffit donc pas de trouver des valeurs des u_i tels que les équations spécialisées en ces u_i aient des solutions dans tous les $\mathbb{Q}_p$.

Le principe de Hasse et l'approximation faible ne valent pas toujours

Il y a – entre autres – des contre-exemples des types suivants.

- $Norm_{K/\mathbb{Q}}(\Xi) = c$ et $K/\mathbb{Q}$ *non cyclique*, par exemple avec $K/\mathbb{Q}$ galoisien de groupe $\mathbb{Z}/2 \times \mathbb{Z}/2$ (Hasse, vers 1930).
- $2y^2 = x^4 - 17$ (courbe de genre 1, Reichardt, Lind, 1940)
- $3x^3 + 4y^3 + 5z^3 = 0$ (courbe de genre 1, Selmer, 1951)
- $y^2 - az^2 = P(t) \neq 0$ (surface géométriquement rationnelle) avec $P(t)$ **réductible**, par exemple (Iskovskikh 1970)

$$y^2 + z^2 = (3 - x^2)(x^2 - 2)$$

- $5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$ (Cassels-Guy, 1966)

L'obstruction de Brauer-Manin

Le groupe de Brauer d'un corps

Soit k un corps, $\mathrm{car}(k) = 0$, et soit $\overline{k}$ une clôture algébrique de k. Soient $a, b \in k^\times$. Les relations

$$i^2 = a, j^2 = b, ij = -ji$$

définissent une k-algèbre $A = (a, b)_k$, de dimension 4 sur k. C'est une "forme tordue" de l'algèbre des matrices 2×2 :

$$A \otimes \overline{k} \simeq M_2(\overline{k}).$$

Pour $k = \mathbf{R}$, $a = b = -1$, ceci n'est autre que l'algèbre des quaternions de Hamilton.

De façon générale, une k-algèbre est appelée algèbre simple centrale s'il existe un entier $n \geq 1$ tel que

$$A \otimes_k \overline{k} \simeq M_n(\overline{k}).$$

Le produit tensoriel de deux k-algèbres centrales simples est une algèbre centrale simple.
On dit que deux telles k-algèbres sont équivalentes s'il existe des entiers $r, s \geq 1$ tels que $M_r(A) \simeq M_s(B)$. Le produit tensoriel définit alors une structure de groupe abélien sur l'ensemble des classes d'équivalence de telles algèbres. C'est le groupe de Brauer du corps k. On le note $\mathrm{Br}(k)$.

Théorie du corps de classes (Hilbert, Takagi, Hasse, ...)
Théorie du corps de classes local

$$\mathrm{Br}\left(\mathbb{Q}_p\right) \simeq \mathbb{Q}/\mathbb{Z}.$$

$$\mathrm{Br}\left(\mathbb{R}\right) = \mathbb{Z}/2$$

On a suite exacte fondamentale de la théorie du corps de classes global (Brauer, Hasse, Noether)

$$0 \to \mathrm{Br}\left(\mathbb{Q}\right) \to \bigoplus_{p \cup \infty} \mathrm{Br}\left(\mathbb{Q}_p\right) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Une conique $x^2 - ay^2 - bt^2 = 0$ sur un corps k (char.$(k) \neq 2$) a un point rationnel si et seulement si la classe de l'algèbre de quaternions $(a, b)_k \in \mathrm{Br}\,(k)$ est nulle.

La formule $\sum_p (a, b)_p = 0$ contient comme cas particulier la loi de réciprocité quadratique.

Le théorème de Legendre peut se reformuler ainsi : Si pour chaque premier p (fini ou infini) $(a, b)_p \in \mathbb{Z}/2 \subset \mathrm{Br}\,(\mathbb{Q}_p)$ s'annule, alors $(a, b) = 0 \in \mathrm{Br}\,(\mathbb{Q})$.

Le groupe de Brauer d'un schéma

Sur une variété algébrique et plus généralement sur un schéma X, les fibrés vectoriels sont les analogues des espaces vectoriels sur un corps.

Les algèbres d'Azumaya sur un schéma sont les analogues naturels des algèbres simples centrales sur un corps.

On peut introduire une relation d'équivalence sur les algèbres d'Azumaya qui étend celle donnée pour les algèbres simples centrales sur un corps. L'ensemble des classes d'équivalence forme un groupe abélien, le groupe de Brauer $\mathrm{Br}\,(X)$ de X.

Soit X un schéma. Pour tout anneau commutatif R il y a un accouplement naturel $X(R) \times \mathrm{Br}\,(X) \to \mathrm{Br}\,(R)$.

La condition de Brauer-Manin pour les points rationnels

Théorème (Manin, 1970). *Soit X une variété projective sur $\mathbb{Q}$. L'image de $X(\mathbb{Q})$ dans $X(A_{\mathbb{Q}}) = \prod_p X(\mathbb{Q}_p)$ est dans le noyau à gauche de l'accouplement (bien défini)*

$$X(A_{\mathbb{Q}}) \times \mathrm{Br}\,(X) \to \mathbb{Q}/\mathbb{Z}$$

$$(\{M_p\}, \alpha) \mapsto \sum_p \mathrm{ev}_A(M_p).$$

On note $X(A_{\mathbb{Q}})^{\mathrm{Br}}$ ce noyau.

L'exemple de Reichardt et Lind du point de vue de l'obstruction de Brauer-Manin

L'équation

$$2y^2 = x^4 - 17 \neq 0$$

définit un ouvert U d'une courbe projective lisse $X/\mathbb{Q}$.

On a $\prod_{p \cup \infty} X(\mathbb{Q}_p) \neq \emptyset$.

Fait : L'algèbre d'Azumaya $(y, 17) \in \mathrm{Br}\,(U)$ s'étend en une algèbre d'Azumaya $A \in \mathrm{Br}\,(X)$.

Pour $p \neq 17$ l'image de $ev_A : X(\mathbb{Q}_p) \to \mathrm{Br}\,(\mathbb{Q}_p) \subset \mathbb{Q}/\mathbb{Z}$ est nulle si $p \neq 17$.

Pour $p = 17$ l'image de $ev_A : X(\mathbb{Q}_{17}) \to \mathrm{Br}\,(\mathbb{Q}_{17}) \subset \mathbb{Q}/\mathbb{Z}$ est $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$.

Donc $X(\mathbb{Q}) = \emptyset$.

L' exemple d'Iskovskikh généralisé, vu du point de vue de l'obstruction de Brauer-Manin

Soit $c \in \mathbb{Z}, c > 0, c$ impair. L'équation

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

définit un ouvert U_c dans une surface projective lisse $X_c/\mathbb{Q}$.
On a $\prod_{p \cup \infty} X_c(\mathbb{Q}_p) \neq \emptyset$.
L'algèbre d'Azumaya $(c - x^2, -1) \in \mathrm{Br}\,(U_c)$ s'étend en $A \in \mathrm{Br}\,(X_c)$.

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

Pour $p \neq 2$, l'image de

$$ev_A : X_c(\mathbb{Q}_p) \to \mathrm{Br}\,(\mathbb{Q}_p) \subset \mathbb{Q}/\mathbb{Z}$$

est nulle.
Pour $p = 2$, cette image est $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$ si et seulement si $c \equiv 3(4)$.
Ainsi : *Si* $c \equiv 3(4)$, *alors* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$, *et donc* $X_c(\mathbb{Q}) = \emptyset$.
Le même calcul montre : *Si* $c \equiv 1(4)$, *alors* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$.
Théorème *Si* $c \equiv 1(4)$ *alors* $X_c(\mathbb{Q}) \neq \emptyset$.
(cas particulier d'un théorème de CT, Coray et Sansuc, 1981)

Un grand nombre de contre-exemples numériques au principe de Hasse *pour les points rationnels* relèvent du cadre proposé par Manin.

On cherche alors des classes de variétés algébriques projectives et lisses sur $\mathbb{Q}$ pour lesquelles l'obstruction de Brauer–Manin *pour les points rationnels* est la seule, i.e. pour X dans la classe, on a l'implication

$$X(A_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset \Longrightarrow X(\mathbb{Q}) \neq \emptyset$$

Ce n'est pas le cas pour toutes les variétés (comme on verra si on a le temps).

Par contre on a la conjecture générale suivante, proposée par CT/Sansuc et Kato/Saito.

Conjecture *Soit X une variété projective et lisse sur $\mathbb{Q}$. Si l'on a $X(A_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$, alors il existe un zéro-cycle de degré 1 sur X.*

Plus généralement :

Conjecture *S'il existe une famille $\{z_p\}$, $z_p \in Z_0^1(X_{\mathbb{Q}_p})$, de zéro-cycles locaux de degré 1 sur X telle que pour tout $A \in \mathrm{Br}\, X$ on ait $\sum_p A(z_p) = 0 \in \mathbb{Q}/\mathbb{Z}$, alors il existe un zéro-cycle global de degré 1 sur X.*
On dit alors : l'obstruction de Brauer-Manin à l'existence d'un zéro-cycle de degré 1 est la seule obstruction.

Les courbes

$g = 0$, ce sont les coniques.

Pour $g \geq 1$, notons $J(X)$ la jacobienne de X. Alors $\mathrm{Br}\, X/\mathrm{Br}\, \mathbb{Q} = H^1(\mathbb{Q}, J)$ est infini.

Pour $g = 1$, si $Ш^1(\mathbb{Q}, J(X))$ est fini (conjecture bien connue), Manin montre (1970) que la suite duale de Cassels-Tate donne

$$X(A_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset \Longrightarrow X(\mathbb{Q}) \neq \emptyset.$$

Plus précisément, on a alors $X = J(X)$ et

$$\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}_{\bullet}$$

où le $\bullet$ signifie qu'on a contracté les composantes connexes.

Pour les courbes de genre $g > 1$, depuis quelques années seulement, on conjecture qu'il en est encore ainsi.

Quelques énoncés théoriques (Skorobogatov et Scharaschkin; Stoll).
Traduction terre à terre en termes d'application de X dans $J(X)$ (Poonen).
Évidence numérique (Bruin et Stoll).

Pour les courbes de genre au moins 2 sur un corps de fonctions d'une variable sur un corps fini, on a un théorème presque général (Poonen et Voloch 2008).

Récent résultat de Bhargava, Gross, Wang (2013):
Pour $g \geq 2$, une proportion positive des courbes hyperelliptiques

$$y^2 = \sum_{i=0}^{2g+2} a_i x^i, \quad a_i \in \mathbb{Z}$$

avec des points dans tous les $\mathbb{Q}_p$ n'a pas de point dans $\mathbb{Q}$, et ce par un calcul de groupe de Selmer qui se traduit en une obstruction de Brauer-Manin.

En ce qui concerne les zéro-cycles sur une courbe X on a, essentiellement par le même argument que Manin (1970):

S'il existe une famille $z_p \in Z_0^1(X_{\mathbb{Q}_p})$ de zéro-cycles de degré 1 telle que pour tout $A \in \mathrm{Br}\, X$ on ait $\sum_p A(z_p) = 0 \in \mathbb{Q}/\mathbb{Z}$, et si $Ш(J(X)$ est fini, alors il existe un zéro-cycle de degré 1 sur X.

Les variétés rationnellement connexes

En dimension arbitraire, les travaux de géométrie algébrique complexe depuis les années 1990 ont a montré que ce sont les bons analogues des courbes de genre zéro (Kollár, Miyaoka, Mori; Campana; Graber, Harris, Starr; de Jong, Starr).

Une variété (projective, lisse) X sur $\mathbb{Q}$ est dite rationnellement connexe si sur le corps $\mathbb{C}$ des complexes, par tout couple de points de $X(\mathbb{C})$ il passe une courbe de genre géométrique zéro.

En dimension 2, toute telle variété sur $/Q$ est $\mathbb{Q}$-birationnelle soit à un fibré en coniques sur une conique soit à une surface de del Pezzo.

Conjecture (CT-Sansuc 1979 en dimension 2) *Pour toute variété projective, lisse, sur $\mathbb{Q}$, rationnellement connexe, on a*

$$\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}.$$

Outre les cas où on connaît le principe de Hasse et l'approximation faible, c'est connu pour :

• les variétés dont un ouvert est un espace homogène d'un groupe algébrique linéaire connexe, avec isotropie géométrique connexe (Sansuc 1981; Borovoi 1996);

• les surfaces fibrées en coniques au-dessus de $\mathbb{P}^1$ avec au plus 4 mauvaises fibres, par exemple $y^2 - az^2 = P(x)$ avec $P(x)$ de degré 4 (CT, Sansuc, Swinnerton-Dyer 1987);

• les intersections lisses de deux quadriques dans $\mathbb{P}^n$, $n \geq 8$ (CT, Sansuc, Swinnerton-Dyer 1985-1987).

• sous l'hypothèse H, pour toute surface fibrée en coniques sur la droite projective.

Outre divers théorèmes de dualité de la théorie du corps de classes, généralisant la suite exacte fondamentale sur le groupe de Brauer, on utilise une combinaison de méthodes :
La *méthode des fibrations*, qui consiste à essayer de trouver des résultats par réduction aux propriétés des fibres, donc de variétés de dimension inférieure. C'est une généralisation des méthodes de Hasse pour les quadriques. Elle a été utilisée par CT-Sansuc-Swinnerton-Dyer 1987, et développée par Skorobogatov et par Harari (1994, 1997).
La *méthode de descente* (CT-Sansuc 1977-1987), qui est un analogue de la descente usuelle sur les points rationnels des courbes. Mais on utilise des torseurs sous des tores au lieu de groupes finis commutatifs. On essaye là de déduire les propriétés arithmétiques des variétés à partir de celles de l'espace total de certains torseurs (torseurs universels).

Il y a aussi une relation entre obstruction de Brauer-Manin et l'existence de certains torseurs sous des tores possédant des points dans tous les $\mathbb{Q}_p$.

On regarde aussi, à l'occasion, ce que donne de façon conditionnelle l'hypothèse H – et maintenant de façon inconditionnelle les résultats de Green, Tao et Ziegler, Browning-Matthiesen.

On regarde enfin ce qu'on pourrait déduire de la finitude de $Ш$ de jacobiennes de courbes – sur les variétés rationnellement connexes, on trouve aussi des courbes de genre > 0.

Exemple originel. On considère une surface X projective et lisse sur $\mathbb{Q}$ "définie" par une équation

$$y^2 - az^2 = \prod_{i=1}^{n} P_i(t) \neq 0$$

avec les $P_i(t)$ irréductibles et premiers entre eux deux à deux.
En utilisant soit la **descente** (torseurs sous des tores) soit le **lemme formel d'Harari** (groupe de Brauer de variétés ouvertes), on montre que l'hypothèse $X(\mathbb{A}_{\mathbb{Q}})^{Br} \neq \emptyset$ **implique** l'existence de $\alpha_i \in \mathbb{Q}^{\times}$ avec $\prod_i \alpha_i = 1$ tels que le sytème

$$y_i^2 - az_i^2 = \alpha_i P_i(t) \neq 0$$

ait des solutions dans tous les $\mathbb{Q}_p$.

Sous l'hypothèse H, le système

$$y_i^2 - az_i^2 = \alpha_i P_i(t) \neq 0$$

avec les $P_i(t)$ irréductibles satisfait le principe de Hasse. Toute solution de ce système sur $\mathbb{Q}$ donne par multiplication naissance à une solution sur $\mathbb{Q}$ de

$$y^2 - az^2 = \prod_{i=1}^{n} P_i(t) \neq 0.$$

L'argument montre en fait que, sous l'hypothèse H, on a $\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$.

Considérons alors X projective et lisse contenant l'ouvert U défini par

$$y^2 - az^2 = c\prod_{i=1}^{n}(t - e_i) \neq 0$$

avec $c \in \mathbb{Q}^\times$ et les $e_i \in \mathbb{Q}$ tous distincts.
Si l'on part d'un point $\{M_p\}$ de $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$ qui est dans U, et de la donnée d'un ensemble fini S de premiers p, on montre de même que l'on peut trouver des $\alpha_i \in \mathbb{Q}^\times$ de produit égal à c tels que la variété V d'équations

$$y_i^2 - az_i^2 = \alpha_i(t - e_i) \neq 0, \quad i = 1, \ldots, n$$

qui se projette sur U par multiplication, admette des solutions $\{N_p\}$ dans tous les $\mathbb{Q}_p$, avec de plus N_p s'envoyant sur M_p pour $p \in S$.

Si on pose $t = u/v$ et qu'on rajoute l'équation $v = y_{n+1}^2 - az_{n+1}^2$, on trouve que V est rétracte (algébrique) de la variété W sur $\mathbb{Q}$ définie par le système

$$y_i^2 - az_i^2 = \alpha_i(u - e_i v), i = 1, \ldots, n; v = y_{n+1}^2 - az_{n+1}^2.$$

Comme le notent Browning, Matthiesen, Skorobogatov ou Harpaz, Skorobogatov, Wittenberg, via les conséquences de Green, Tao et Ziegler le principe de Hasse et l'approximation faible valent pour un tel système. On en déduit :

$$\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}.$$

En particulier les points rationnels sont Zariski denses sur la surface $y^2 - az^2 = c\prod_{i=1}^{2n}(t - e_i)$, ce qui était un problème ouvert depuis longtemps.

De façon plus générale, on a le

Théorème (Harpaz, Skorobogatov, Wittenberg 2013)
Soient $K_i/\mathbb{Q}$, $i = 1, \ldots, r$ des extensions cycliques de $\mathbb{Q}$ et soient $e_i \in \mathbb{Q}$ et $b_i \in \mathbb{Q}^\times$ pour $i = 1, \ldots, r$. Alors le principe de Hasse et l'approximation faible valent pour les solutions rationnelles du système

$$\mathrm{Norm}_{K_i/\mathbb{Q}}(\Xi_i) = b_i(t - e_i) \neq 0.$$

Voici un énoncé de fibration idéal qu'on aimerait avoir

(??) *Soit X une $\mathbb{Q}$-variété projective et lisse équipée d'un morphisme $p : X \to \mathbb{P}^1_{\mathbb{Q}}$ dont la fibre générique est une variété rationnellement connexe. Supposons que pour les fibres lisses $X_M = p^{-1}(M)$ avec M un point $\mathbb{Q}$-rationnel, l'adhérence de $X_M(\mathbb{Q})$ dans $X_M(\mathbb{A}_{\mathbb{Q}})$ est $X_M(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$. Alors $\overline{X(\mathbb{Q})}^{top} = X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$.*

Voici deux cas où c'est "connu".

• Le cas où les fibres de p sur $\mathbb{A}^1 \subset \mathbb{P}^1$ sont géométriquement intègres : c'est l'un des principaux théorèmes de la thèse d'Harari (1994). C'est pour établir ce résultat qu'il développa le "lemme formel".

• **Sous l'hypothèse H**, avec l'hypothèse supplémenaire de **scindage abélien** pour p, c'est-à-dire que pour tout point fermé $M \in \mathbb{P}^1_{\mathbb{Q}}$ la fibre X_M contient une composante Y de multiplicité 1 qui est "déployée" sur une extension *abélienne* du corps résidulel $\mathbb{Q}(M)$, et sous l'hypothèse plus forte que principe de Hasse et approximation faible valent pour les fibres.
(CT-Skorobogatov-Swinnerton-Dyer 1998, généralisation de résultats antérieurs de CT-Sansuc 1979, Serre, Swinnerton-Dyer).
Exemple : le scindage abélien est évident pour les fibrations en coniques.

On aimerait combiner les deux approches pour traiter les variétés birationnellement fibrées sur $\mathbb{P}^1$ en espaces homogènes de groupes algébriques linéaires connexes.
On a dans cette direction des résultats particuliers et récents de Browning et Heath-Brown, de Dasheng Wei, Yongqi Liang, A. Smeets, U. Derenthal, certains reposant sur la méthode du cercle.

Harpaz et Wittenberg (en cours, septembre-octobre 2013) ont réussi dans un grand nombre de nouveaux cas à **se débarrasser de l'hypothèse de scindage abélien** et à combiner les approches.
Harpaz et Wittenberg vont donner des cas particuliers où les seules fibres non lisses sont situées sur des points $\mathbb{Q}$-rationnels et où l'on peut donc, via Green-Tao-Ziegler, se débarrasser aussi de l'hypothèse H.

Voici un énoncé inconditionnel et général qu'ils ont obtenu en ce qui concerne les zéro-cycles de degré 1, en combinant leur approche avec l'astuce de Salberger :

Théorème (Harpaz et Wittenberg 2013) *Soit X une $\mathbb{Q}$-variété projective et lisse équipée d'un morphisme $p : X \to \mathbb{P}^1_{\mathbb{Q}}$ dont la fibre générique est une variété rationnellement connexe. Supposons que pour les fibres lisses $X_M = p^{-1}(M)$ avec M un point fermé de $\mathbb{P}^1_{\mathbb{Q}}$, l'adhérence de $X_M(\mathbb{Q}(M))$ dans $X_M(\mathbb{A}_{\mathbb{Q}(M)})$ est $X_M(\mathbb{A}_{\mathbb{Q}(M)})^{Br}$. S'il existe une famille $z_p \in Z_0^1(X_{\mathbb{Q}_p})$ de zéro-cycles de degré 1 telle que pour tout $A \in \mathrm{Br}\, X$ on ait $\sum_p A(z_p) = 0 \in \mathbb{Q}/\mathbb{Z}$, alors il existe un zéro-cycle de degré 1 sur X.*

Yongqi Liang et Dasheng Wei avaient déjà chacun obtenu des résultats partiels mais significatifs dans cette direction.

On aurait pu rêver d'avoir un théorème de fibration "idéal" du type ci-dessus sur les points rationnels sans restriction sur la géométrie de la fibre générique. On fibrerait alors toute surface par une fibration disons de Lefschetz, et on se ramènenait au cas conjecturalement connu des courbes ! Mais ça ne saurait marcher en général, car il existe des variétés pour lesquelles l'obstruction de Brauer-Manin au principe de Hasse n'est pas la seule obstruction pour les points rationnels.

On connaît des $X/\mathbb{Q}$ avec $X(\mathbb{Q}) = \emptyset$ mais $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \neq \emptyset$ parmi :

- Les surfaces biellipticques (Skorobogatov, 1999)
- Les variétés fibrées en surfaces de Châtelet ($y^2 - az^2 = P_4(x)$) au-dessus d'une courbe de genre $g \geq 1$ (Poonen, 2010).

Ces exemples sont expliqués par "l'obstruction de Brauer-Manin étale" et la descente "non commutative" (Skorobogatov, Harari, Demarche). Ce n'est pas le cas pour les exemples suivants :

- Certaines surfaces de type général construites par Harpaz et Skorobogatov (2012).
- Des surfaces fibrées en coniques au-dessus d'une courbe de genre $g \geq 1$ (CT, Pál, Skorobogatov 2013).

Swinnerton-Dyer (1995) a initié une technique, ensuite développée dans plusieurs articles par CT, Skorobogatov et lui (1998) et par Wittenberg (2006), méthode qui donne des résultats conditionnels sur certaines variétés fibrées en courbes de genre 1 ou en produit de telles courbes.

Tous les résultats dans cette direction supposent la finitude des groupes de Tate-Shafarevich des courbes elliptiques, en tout cas pour toutes les courbes dans des familles algébriques de courbes.

Modulo la finitude des groupes de Tate-Shafarevich, Swinnerton-Dyer (2001) a ainsi établi le principe de Hasse pour beaucoup de surfaces cubiques diagonales sur $\mathbb{Q}$, avec comme conséquence le principe de Hasse sur $\mathbb{Q}$ pour toutes les hypersurfaces cubiques diagonales dans $\mathbb{P}^4$:

$$\sum_{i=0}^{4} a_i x_i^3 = 0.$$

Certains des résultats sont encore plus conditionnels : ils reposent à la fois sur la finitude de Tate-Shafarevich et sur l'hypothèse H. On obtient ainsi des résultats conditionnels sur certaines surfaces $K3$ (CT, Skorobogatov, Swinnerton-Dyer 1998; Swinnerton-Dyer 2000; Skorobogatov, Swinnerton-Dyer 2005). Pour les surfaces $K3$, on pourrait rêver que l'obstruction de Brauer-Manin au principe de Hasse soit toujours la seule obstruction.

Supposons à la fois la finitude de Tate-Shafarevich et l'hypothèse H.
Un résultat frappant est celui de Wittenberg (2006-2007), qui est l'analogue du résultat de Swinnerton-Dyer sur les surfaces cubiques diagonales, mais pour presque toutes les intersections lisses de deux quadriques dans $\mathbb{P}^4$, pas forcément simultanément diagonales, avec la conclusion que le principe de Hasse vaut pour les intersections lisses quelconques de deux quadriques dans $\mathbb{P}^n$, $n \geq 5$ – à comparer avec les résultats inconditionnels connus ($n \geq 8$, CT-Sk-SwD 1987; $n = 7$, Heath-Brown 2013).