Lois de réciprocité et solutions entières d'équations polynomiales

J.-L. Colliot-Thélène

Colloquium de l'IRMAR, Rennes, 14 novembre 2005

Congruences, corps locaux

Soit $f(x_1, \cdots, x_n)$ un polynôme à coefficients entiers. On s'intéresse de tout temps à l'existence de solutions entières (parfois de solutions entières primitives) de l'équation

$$f(x_1, \cdots, x_n) = 0.$$

La réponse négative au dixième problème de Hilbert n'a pas enlevé tout attrait à ce problème : on cherche des classes d'équations pour lesquelles on aurait une méthode pour décider de l'existence de solutions.

Il y a des impossibilités manifestes.

On ne peut résoudre $x^2 + y^2 + 1 = 0$ sur $\mathbf{R}$.

Il y a d'autres impossibilités au moyen de congruences. Ainsi $x^2+y^2-3z^2 = 0$ n'a pas de solution primitive, comme on le voit soit en utilisant une congruence modulo 9 soit en utilisant une congruence modulo 4.

Pour tout p premier, l'équation $x^3 + py^3 + p^2z^3 = 0$ n'a pas de solution non triviale, comme on voit par une congruence modulo p^3.

Hensel expliqua comment exprimer les conditions de congruence de manière agréable, parallèle aux conditions réelles. Pour chaque p premier on construit un anneau commutatif intègre $\mathbf{Z}_p$, de corps des fractions un corps $\mathbf{Q}_p$ qui est le complété de $\mathbf{Q}$ pour la métrique p-adique.

Une équation comme ci-dessus a une solution (primitive) dans $\mathbf{Z}_p$ si et seulement si elle a une solution (primitive) modulo toute puissance de p.

Si l'on note $X(R)$ l'ensemble des solutions à coordonnées dans un anneau commutatif R d'une équation comme ci-dessus, on a les inclusions naturelles

$$X(\mathbf{Z}) \subset \prod_p X(\mathbf{Z}_p)$$

$$X(\mathbf{Q}) \subset \prod_p X(\mathbf{Q}_p)$$

Ici p prend aussi la valeur ∞, avec la convention $\mathbf{Z}_\infty = \mathbf{Q}_\infty = \mathbf{R}$.

Le théorème de Legendre

Théorème (Legendre, 1785). *Soit $q(x, y, z)$ une forme quadratique entière. Si l'équation $q(x, y, z) = 0$ a des solutions non triviales dans tous les $\mathbf{Z}_p$ et dans $\mathbf{R}$, alors elle a une solution non triviale dans $\mathbf{Z}$.*

Deux observations.

(a) La démonstration, qui relève de la géométrie des nombres, donne une borne supérieure sur la taille de la plus petite solution.

(b) Les démonstrations n'utilisent pas toute la force de l'hypothèse : on peut se dispenser d'utiliser l'hypothèse 2-adique. Ou bien l'on peut se dispenser d'utiliser l'hypothèse sur les réels.

Loi de réciprocité quadratique (theorema fundamentale)

p premier impair, a entier premier à p,
Symbole de Legendre $(a/p) = \pm 1$
$(a/p) = 1$ si et seulement si a est un carré modulo p.

p, q premiers impairs

$$(p/q)(q/p) = (-1)^{(p-1)/2.(q-1)/2}$$

prédit indépendamment par Euler et Legendre (1785); première démonstration par Gauß le 18 avril 1796.

Premier complément

$$(-1/p) = (-1)^{(p-1)/2}$$

Soit : -1 est un carré modulo p premier impair si et seulement si $p \equiv 1(4)$.

Deuxième complément

$$(2/p) = (-1)^{(p^2-1)/8}$$

Soit : 2 est un carré modulo p premier impair si et seulement si $p \equiv \pm 1(8)$.

Le principe de Hasse pour les formes quadratiques en au moins 4 variables

Théorème (Minkowski, Hasse 1920). *Soit $q(x_1, \cdots, x_n)$ une forme quadratique entière. Si l'équation $q(x_1, \cdots, x_n) = 0$ a des solutions non triviales dans tous les $\mathbf{Z}_p$ et dans $\mathbf{R}$, alors elle a une solution non triviale dans $\mathbf{Z}$.*

Pour la démonstration de Hasse, un point clé est le passage de 3 à 4 variables. La démonstration de Hasse utilise ici le théorème de Dirichlet sur les premiers dans une progression arithmétique.

A la suite de ce théorème, on se demanda dans quelle mesure ce "principe de Hasse" vaut pour d'autres classes d'équations.

Je ne parlerai pas ici de la méthode du cercle, si ce n'est pour dire que cette méthode analytique donne de bons résultats pour les hypersurfaces quand le nombre de variables est grand par rapport au degré.

Un record ici est le théorème de Hooley (suivant un travail de Heath-Brown) :

Le principe de Hasse vaut pour les formes cubiques non singulières en au moins 9 variables.

(Mais on conjecture que c'est le cas dès que l'on a 5 variables.)

Ceci dit, on dispose de nombreux contre-exemples au principe de Hasse.

Un exemple de Lind (1940)

Il s'agit d'une courbe de genre 1 ayant des points dans tous les $\mathbf{Q}_p$ et $\mathbf{R}$ mais pas dans $\mathbf{Q}$.

$$2y^2 = x^4 - 17, \;\; x, y \in \mathbf{Q}$$

$$2u^2 = v^4 - 17w^4 \neq 0, \;\; u, v, w \in \mathbf{Z}, \;\; (v, w) = 1$$

Argument modulo 17^2 : on voit que 17 ne divise pas u. Comme 2 n'est pas une puissance 4ème modulo 17, ceci implique que u n'est pas un carré modulo 17.

p premier impair, p divise u (donc $p \neq 17$)
$\Longrightarrow$ 17 carré modulo p
$\Longrightarrow$(réciprocité quadratique) p est un carré modulo 17.
Aussi, 2 est un carré modulo 17. D'où u carré modulo 17.

Contradiction.

Un exemple d'Iskovskikh (1971)

Il s'agit d'une surface "rationnelle" ayant des points dans tous les $\mathbf{Q}_p$ et $\mathbf{R}$.

$$y^2 + z^2 = (3 - x^2)(x^2 - 2) \;\; x, y, z \in \mathbf{Q}$$

Solution dans $\mathbf{Q}$?

$$u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0, \;\; u, v, x, y \in \mathbf{Z}, (x, y) = 1$$

$$(3y^2 - x^2, x^2 - 2y^2) = 1$$

On voit que le couple $(3y^2 - x^2, x^2 - 2y^2)$ peut prendre l'une des valeurs suivantes modulo 4 :

$$(2, -1), (-1, 1), (3, 2)$$

On a $3y^2 - x^2 > 0, \;\; x^2 - 2y^2 > 0$.

Si p^{2n+1} divise exactement $3y^2 - x^2$ ou $x^2 - 2y^2$ alors p^{2n+1} divise exactement $u^2 + v^2$ donc -1 est un carré mod. p, donc (loi de réciprocité, premier complément) p congru à 1 mod. 4.

Ainsi $(3y^2 - x^2, x^2 - 2y^2)$ prend l'une des valeurs suivantes modulo 4 :

$$(1, 1), (2, 1), (1, 2)$$

Contradiction.

Un exemple de Borovoi et Rudnick (1995)

$$q(x,y,z) = -9x^2 + 2xy + 7y^2 + 2z^2$$

$$-9x^2 + 2xy + 7y^2 + 2z^2 = 1$$

soit encore

$$(x-y)^2 + 8(x-y)(x+y) = 2z^2 - 1$$

Solution sur $\mathbf{Q}$

$$q(-1/2, 1/2, 1) = 1$$

donc sur tous $\mathbf{Z}_p$ pour $p \neq 2$.

Solution sur $\mathbf{Z}_2$, $q(4,1,1) = -127 \equiv 1(8)$.

Solution avec $(x,y,z) \in \mathbf{Z}$?

Une discussion des congruences modulo des puissances de 2 montre

$$x - y \equiv \pm 3(8)$$

Si p premier divise $x-y$, alors p divise $2z^2 - 1$
$\Longrightarrow$ p impair et 2 carré mod. p
$\Longrightarrow$ (second complément à la loi de réciprocité) $p \equiv \pm 1(8)$.
Ainsi $x - y \equiv \pm 1(8)$.
Contradiction.

Groupe de Brauer d'un corps

Soit k un corps de caractéristique nulle, $\overline{k}$ une clôture algébrique.

Soient $a, b \in k^*$. La k-algèbre A définie par les relations

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

est de dimension 4 sur k, elle satisfait $A \otimes \overline{k} \simeq M_2(\overline{k})$. L'exemple classique est celui des quaternions de Hamilton : $k = \mathbf{R}$, $a = b = -1$.

De façon générale, on appelle k-algèbre simple centrale une k-algèbre A telle qu'il existe un entier $n \geq 1$ avec $A \otimes \overline{k} \simeq M_n(\overline{k})$. Le produit tensoriel de deux k-algèbres simples centrales est une k-algèbre simple centrale. Si l'on dit que deux telles k-algèbres A et B sont équivalentes s'il existe des entiers $r, s \geq 1$ avec $M_r(A) \simeq M_s(B)$, alors le produit tensoriel induit une structure de groupe abélien sur l'ensemble des classes d'équivalence : c'est le groupe de Brauer de k. On le note $\mathrm{Br}(k)$.

Corps de classes

Corps de classe local

$$\mathrm{Br}(\mathbf{Q}_p) \simeq \mathbf{Q}/\mathbf{Z}.$$

$$\mathrm{Br}(\mathbf{R}) = \mathbf{Z}/2$$

Suite exacte fondamentale en théorie du corps de classes global

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

La conique $x^2 - ay^2 - bt^2 = 0$ sur le corps k (de car. différente de 2) a un point rationnel si et seulement si la classe de l'algèbre de quaternions $(a, b) \in \mathrm{Br}(k)$ (définie par $i^2 = a, j^2 = b, ij = -ji$) est nulle.

Le théorème de Legendre se traduit : $(a, b)_p \in \mathbf{Z}/2 \subset \mathrm{Br}(\mathbf{Q}_p)$ nul pour tout premier p (fini ou non) implique $(a, b) = 0 \in \mathrm{Br}(\mathbf{Q})$.

Comme on a $\sum_p (a, b)_p = 0$, il suffit de connaître la nullité pour tous les premiers p (p fini ou infini) sauf l'un d'entre eux.

Loi de réciprocité quadratique (équation $X^2 - pY^2 - qZ^2 = 0$)
p, q premiers impairs, $\sum_l (p, q)_l = 0$.
Car
$(p, q)_l = 0$ si $l \neq 2, p, q$,
$(p, q)_q = 0$ si et seulement si $(p/q) = 1$,
$(p, q)_p = 0$ si et seulement si $(q/p) = 1$
$(2, p)_2 = 0$ si et seulement si $(-1)^{(p-1)/2.(q-1)/2} = 1$.

Premier complément (équation $X^2 + Y^2 - pZ^2 = 0$)
p premier impair, $\sum_l (-1, p)_l = (-1, p)_p + (-1, p)_2 = 0$.

Deuxième complément (équation $X^2 - 2Y^2 - pZ^2 = 0$)
p premier impair, $\sum_l (2, p)_l = (2, p)_p + (2, p)_2 = 0$.

Groupe de Brauer d'un schéma

Sur une variété algébrique, et plus généralement sur un schéma, la notion de fibré vectoriel généralise celle d'espace vectoriel sur un corps. De même, la notion d'algèbre d'Azumaya sur un schéma généralise celle d'algèbre simple centrale sur un corps. On introduit une relation d'équivalence entre les algèbres d'Azumaya, qui mène à la définition du groupe de Brauer $\mathrm{Br}(X)$ d'un schéma. Celui-ci a de bonnes propriétés fonctorielles.

En particulier, si X est un $\mathbf{Z}$-schéma, on a un accouplement

$$X(R) \times \mathrm{Br}(X) \to \mathrm{Br}(R)$$

pour tout anneau commutatif R.

Les conditions de Brauer-Manin

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

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

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

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

On a la variante entière :
Proposition. *Soit X un $\mathbf{Z}$-schéma de type fini. L'image de $X(\mathbf{Z})$ dans $\prod_p X(\mathbf{Z}_p)$ est dans le noyau de l'accouplement (bien défini)*

$$\prod_p X(\mathbf{Z}_p) \times \mathrm{Br}(X_{\mathbf{Q}}) \to \mathbf{Q}/\mathbf{Z}$$

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

On note ce noyau $(\prod_p X(\mathbf{Z}_p))^{\mathrm{Br}(X_{\mathbf{Q}})}$.

Interprétation à la Brauer-Manin du premier exemple

L'équation

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

définit un ouvert dense U d'une courbe X projective et lisse sur $\mathbf{Q}$.
On a $\prod_{p \cup \infty} X(\mathbf{Q}_p) \neq \emptyset$.
L'algèbre d'Azumaya $(y, 17) \in \mathrm{Br}(U)$ vient de $A \in \mathrm{Br}(X)$.
L'image de

$$ev_A : X(\mathbf{Q}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$$

est nulle si $p \neq 17$, elle coïncide avec $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ si $p = 17$.
Donc $X(\mathbf{Q}) = \emptyset$.

Interprétation à la Brauer-Manin du second exemple

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

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

définit un ouvert dense U d'une surface X projective et lisse sur $\mathbf{Q}$.
On a $\prod_{p \cup \infty} X(\mathbf{Q}_p) \neq \emptyset$.
L'algèbre d'Azumaya $(c - x^2, -1) \in \mathrm{Br}(U)$ vient de $A \in \mathrm{Br}(X)$.
L'image de

$$ev_A : X(\mathbf{Q}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$$

est nulle si $p \neq 2$.
Pour $p = 2$ elle coïncide avec $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ si et seulement si $c \equiv 3(4)$.
Donc $X(\mathbf{Q}) = \emptyset$ si $c \equiv 3(4)$.

Théorème (cas particulier de CT/Coray/Sansuc 1981) $c \equiv 1(4) \Longrightarrow X(\mathbf{Q}) \neq \emptyset$.

Interprétation à la Brauer-Manin d'une famille d'exemples dans le style du troisième exemple

Soit n, m, k des entiers positifs, avec $(n, m) = 1$.
L'équation

$$m^2x^2 + n^{2k}y^2 - nz^2 = 1$$

soit encore

$$(1 + n^k y)(1 - n^k y) = m^2x^2 - nz^2$$

à résoudre avec $(x, y, z) \in \mathbf{Z}$ a été considérée par F. Xu et R. Schulze-Pillot. Soit $X/\mathbf{Z}$ le schéma défini par l'équation ci-dessus.

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

L'algèbre d'Azumaya $(1 + n^k y, n)$ définie sur l'ouvert $U_{\mathbf{Q}} \subset X_{\mathbf{Q}}$ d'équation $1 + n^k y \neq 0$ provient d'un élément $A \in \mathrm{Br}(X_{\mathbf{Q}})$.

L'image de

$$ev_A : X(\mathbf{Z}_p) \to \mathrm{Br}(\mathbf{Q}_p) \subset \mathbf{Q}/\mathbf{Z}$$

est nulle si $p \neq 2$.

Pour $p = 2$ cette image coïncide avec $\{1/2\} \subset \mathbf{Q}/\mathbf{Z}$ si et seulement si

(i) 2 divise exactement m et $n \equiv 5(8)$
ou
(ii) 4 divise m et $n \equiv 3$ ou $5(8)$

Donc $X(\mathbf{Z}) = \emptyset$ si on est dans l'un des deux cas ci-dessus.

Théorème (F. Xu et R. Schulze-Pillot, 2004). *Dans les autres cas,* $X(\mathbf{Z}) \neq \emptyset$.
Une autre démonstration est obtenue au moyen du théorème général suivant.

Théorème. *Soit $q(x_1, \cdots, x_n)$une forme quadratique de rang n, à coefficients entiers, indéfinie (signe variable sur les réels), et soit $a \in \mathbf{Z}$, $a \neq 0$. Soit $X/\mathbf{Z}$ le $\mathbf{Z}$-schéma défini par $q(x_1, \cdots, x_n) = a$. Supposons $\prod_p X(\mathbf{Z}_p) \neq \emptyset$.*

(a) Pour $n \geq 4$ l'équation $q(x_1, \cdots, x_n) = a$ a une solution dans $\mathbf{Z}$.

(b) Pour $n = 3$, supposons $-a.det(q)$ non carré.

On a $\mathrm{Br}(X_{\mathbf{Q}})/\mathrm{Br}(\mathbf{Q}) = \mathbf{Z}/2$. Soit $A \in \mathrm{Br}(X_{\mathbf{Q}})$ un générateur. On a $X(\mathbf{Z}) \neq \emptyset$ si et seulement si l'application

$$\prod_p X(\mathbf{Z}_p) \to \mathbf{Q}/\mathbf{Z}$$

donnée par

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

a 0 dans son image.

L'énoncé (a) date des années 1950 (Eichler; Kneser, Watson).

L'énoncé (b) est une variante (CT/F. Xu, 2005) d'un énoncé de Borovoi et Rudnick (1995). Le point clé est le théorème d'approximation forte pour le groupe des spineurs d'une forme quadratique indéfinie, et la présentation d'une quadrique affine $q = a$ sur $\mathbf{Q}$, possédant un point rationnel, comme un espace G/T, où G est le groupe des spineurs de q et T est un tore algébrique de dimension 1.

On calcule A de la façon suivante. Soit M un point $\mathbf{Q}$-rationnel sur $q(x, y, z) = a$. Soit $l(x, y, z) = 0$ l'équation du plan tangent à la quadrique affine $X_{\mathbf{Q}}$ en M. On prend pour A l'algèbre de quaternions $(l(x, y, z), -ad)$.

Espaces homogènes de groupes linéaires connexes

Le principe de Hasse pour les espaces principaux homogènes de groupes semi-simples simplement connexes (Hasse, Landherr, Eichler, Kneser, Harder, Chernousov) a pour conséquence les énoncés suivants.

Théorème (Harder, 1970) *Soit $X/\mathbf{Q}$ une variété projective et lisse espace homogène d'un groupe linéaire connexe. Le principe de Hasse vaut pour X.*

Cet énoncé de Harder généralise le théorème de Hasse sur les quadriques.

Théorème (Borovoi, 1996). *Soit $X/\mathbf{Q}$ une variété projective et lisse contenant un ouvert U qui est un espace homogène d'un groupe linéaire connexe. Soit H le groupe d'isotropie, i.e. le $\overline{\mathbf{Q}}$-groupe algébrique fixant un $\overline{\mathbf{Q}}$-point de U. Si ce groupe est connexe ou abélie, alors $X(\mathbf{Q})$ est dense dans $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$. En particulier, $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ implique $X(\mathbf{Q}) \neq \emptyset$.*

Cet énoncé de Borovoi généralise des résultats de Sansuc (1981).

Une conséquence est le cas $n = 4$ de l'énoncé suivant :

Une intersection lisse de 2 quadriques dans $\mathbf{P}^n_{\mathbf{Q}}$ ($n \geq 4$) qui contient un ensemble de deux droites conjuguées satisfait le principe de Hasse.

La méthode des sections hyperplanes permet de passer du cas $n = 4$ au cas $n > 4$.

Le principe de Hasse vaut pour les surfaces cubiques

$$ax^3 + by^3 + cz^3 + dt^3 = 0$$

lorsque ab/cd est un cube.

Courbes de genre 1

Exemples : cubiques planes non singulères, intersections lisses non singulières de deux quadriques dans $\mathbf{P}^3$.

Une courbe elliptique est une courbe de genre 1 munie d'une structure de groupe. L'existence d'une telle structure sur une courbe de genre 1 est équivalente à celle d'un point rationnel.

A toute courbe projective, lisse, de genre 1 définie sur $\mathbf{Q}$ on associe une courbe elliptique $J = J(X)$ sur $\mathbf{Q}$, la jacobienne de X. La courbe X est un espace principal homogène sous J. L'ensemble des classes d'isomorphie de courbes X ayant même jacobienne J est un groupe, le groupe de Weil-Châtelet $WC(J)$. La classe de X est nulle si et seulement si $X(\mathbf{Q}) \neq \emptyset$.

Le groupe de Tate-Shafarevich $Sha(J) \subset WC(J)$ est le sous-groupe formé des classes de courbes ayant des points dans tous les $\mathbf{Q}_p$.

Hypothèse fondamentale *Le groupe $Sha(J)$ est fini.*

Proposition (Manin 1970). *Sous cette hypothèse, si $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$, alors $X(\mathbf{Q}) \neq \emptyset$.*

L'énoncé vaut sous la simple hypothèse $X(A_{\mathbf{Q}})^{\mathrm{Br}_\omega(X)} \neq \emptyset$, où $\mathrm{Br}_\omega(X) \subset \mathrm{Br}(X)$ consiste en les classes partout localement constantes.

Cassels et Tate ont montré que si le groupe $Sha(J)$ est fini, alors il est muni d'une forme alternée non dégénérée. Ceci implique que le groupe $Sha(J)$ est une somme directe de groupes de la forme $(\mathbf{Z}/n)^2$. En particulier, pour tout entier r, l'ordre du sous-groupe annulé par r est un carré.

On en tire le modeste principe de Hasse suivant :

Sous la conjecture fondamentale, si une courbe $X/\mathbf{Q}$ de genre 1 a des points dans tous les $\mathbf{Q}_p$, si sa classe dans $Sha(J(X))$ est annulée par le premier l et que l'ordre de la l-torsion de $Sha(J(X))$ est au plus l, alors $X(\mathbf{Q}) \neq \emptyset$.

Courbes de genre plus grand que 1

Soit $X/\mathbf{Q}$ une courbe projective, lisse, de genre $g \geq 2$. A toute telle courbe on associe une variété abélienne J de dimension g. D'après Faltings, $X(\mathbf{Q})$ est fini.

Théorème *Supposons $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$, et supposons le groupe de Tate-Shafarevich de J fini.*

(a) Il existe alors un plongement $X \subset J$ défini sur $\mathbf{Q}$

(b) Pour ce plongement $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \subset J(A_{\mathbf{Q}})$ est contenu dans l'adhérence de $J(\mathbf{Q})$ dans $J(A_{\mathbf{Q}})$.

(c) (Scharaschkin) Si $J(\mathbf{Q})$ est fini, alors $X(\mathbf{Q}) = X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$; en particulier $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ implique $X(\mathbf{Q}) \neq \emptyset$.

(Enoncé un peu imprécis aux places réelles.)

Question (Skorobogatov) *Pour X une courbe projective et lisse quelconque, est-il vrai que $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ implique $X(\mathbf{Q}) \neq \emptyset$?*

Trois types de travaux dans cette direction.

Vérification que les contre-exemples au principe de Hasse connus parmi certaines courbes de Shimura s'expliquent à la Brauer-Manin (Skorobogatov, Siksek, Rotger, Yafaev).

Etude systématique de courbes de genre 2 (Flynn, 2004) : on cherche à établir $X(\mathbf{Q}) = \emptyset$ en étudiant l'intersection de $X(\mathbf{F}_p)$ avec l'image de $J(\mathbf{Q})$ dans $J(\mathbf{F}_p)$ (avec un p ou avec plusieurs p simultanément).

(2005) Explication à la Brauer-Manin de certains contre-exemples au principe de Hasse : si l'on dispose d'un $\mathbf{Q}$-morphisme dominant $X \to E$, où E est une courbe de genre 1 avec un nombre fini de points rationnels et il n'existe pas de point rationnel de X au-dessus de ces points, $X(A_{\mathbf{Q}}) \neq \emptyset$ et $Sha(E)$ fini. (Siksek, CT, cas spéciaux; cas général dû à Stoll, via des résultats de Serre sur l'action de Galois sur les points de torsion).

Pinceaux de courbes de genre 0

Théorème (CT/Sansuc 1978, Serre, CT/Swinnerton-Dyer) *Soit $X/\mathbf{Q}$ une surface projective et lisse birationnelle à une surface d'équation affine*

$$a(t)x^2 + b(t)y^2 + c(t) = 0$$

($(a(t), b(t), c(t)$ polynômes non nuls). Sous l'hypothèse de Schinzel, $X(\mathbf{Q})$ est dense dans $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)}$.

Hypothèse de Schinzel *Soient $P_1(t), \cdots, P_m(t)$ des polynômes irréductibles à coefficients entiers, de coefficient dominant positif. Supposons qu'aucun premier ne divisent tous les $\prod_i P_i(n)$ lorsque n varie. Alors il existe une infinité d'entiers n tels que chaque $P_i(n)$ soit un nombre premier.*

Contient l'hypothèse des nombres premiers jumeaux.

On sait démontrer de façon inconditionnelle le théorème ci-dessus dans le cas où la fibration en coniques (donnée par le paramètre t) a au plus 5 fibres géométriques singulières (CT/Sansuc/Swinnerton-Dyer 1984, CT 1990, Salberger/Skorobogatov 1991). Deux méthodes : la descente (torseurs universels, CT/Sansuc) et une méthode via les zéro-cycles (Salberger).

Par une méthode de fibration, ceci permit de montrer (1984) :

Théorème. *Soit $n \geq 8$. Si une intersection lisse de deux quadriques dans $\mathbf{P}^n_{\mathbf{Q}}$ a un point réel, alors elle a un point rationnel.*

Résultats antérieurs : Mordell ($n \geq 12$); Swinnerton-Dyer ($n \geq 10$)

Pinceaux de courbes de genre 1

Partant du cas très particulier de principe de Hasse pour une courbe de genre 1 mentionné plus haut, Swinnerton-Dyer en 1995 a initié une nouvelle méthode. Elle a été poursuivie par lui et d'autres (CT/Skorobogatov/SwD, Bender/SwD, SwD, CT, Skorobogatov/SwD, Wittenberg).

Citons simplement les résultats les plus frappants obtenus par cette méthode.

Théorème (Swinnerton-Dyer, 2000) *Soient $a_i, i = 0, \cdots, 3$ des éléments de $\mathbf{Q}^*$ dont le produit est un carré. Soit $X \subset \mathbf{P}^3_{\mathbf{Q}}$ la surface quartique définie par l'équation*

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

Supposons :

(i) La torsion 2-primaire des groupes de Tate-Shafarevich des courbes elliptiques définies sur $\mathbf{Q}$ est finie;

(ii) L'hypothèse de Schinzel est satisfaite.

(iii) Le produit des a_i n'est pas dans $\mathbf{Q}^{*4}$ et aucun des $\pm a_i a_j$ pour $i \neq j$ n'est un carré.

(iv) L'ensemble $X(A_{\mathbf{Q}})^{\mathrm{Br}}$ est non vide.

Alors X possède des points $\mathbf{Q}$-rationnels.

Les deux énoncés suivants n'utilisent pas l'hypothèse de Schinzel.

Théorème (Swinnerton-Dyer, 2001) *Soient $a_i \in \mathbf{Z}, i = 0, \cdots, 3$ des entiers non nuls, sans facteur commun, chacun d'entre eux non divisible par un cube. Soit $X \subset \mathbf{P}^3_{\mathbf{Q}}$ la surface cubique diagonale donnée par*

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

Supposons que sur toute extension quadratique k de $\mathbf{Q}$, la partie 3-primaire des groupes de Tate-Shafarevich des courbes elliptiques d'équation $X^3 + Y^3 = aT^3$ ($a \in k^*$) est finie. Supposons satisfaite l'une des hypothèses :

(i) Il existe un premier $p \neq 3$ divisant a_0 mais aucun des autres a_i et il existe un premier $q \neq 3$ divisant a_1 mais aucun des autres a_i.

(ii) Il existe un premier $p \neq 3$ divisant a_0 mais aucun des autres a_i, et les classes de a_1, a_2, a_3 dans $\mathbf{F}_p^*/\mathbf{F}_p^{*3}$ ne sont pas toutes égales.

Alors le principe de Hasse vaut pour X : Si X a des points rationnels dans tous les complétés de $\mathbf{Q}$, alors X a des points $\mathbf{Q}$-rationnels.

Théorème (Swinnerton-Dyer 2001) *Supposons que sur toute extension quadratique k de $\mathbf{Q}$, la partie 3-primaire des groupes de Tate-Shafarevich des courbes elliptiques d'équation $X^3 + Y^3 = aT^3$ ($a \in k^*$) est finie. Alors, sur le corps $\mathbf{Q}$ des rationnels, pour tout $n \geq 4$, le principe de Hasse vaut pour toute hypersurface cubique diagonale*

$$\sum_{i=0}^{n} a_i T_i^3 = 0.$$

Olivier Wittenberg vient d'achever de façon spectaculaire un programme commencé par Swinnerton-Dyer et Bender, et poursuivi en partie par moi-même. La démonstration des résultats ci-dessous utilise aussi un résultat récent de D. Harari.

Il a montré :

Théorème (Wittenberg, 2005) *Soit $X \subset \mathbf{P}^4_{\mathbf{Q}}$ une intersection lisse de deux quadriques définie par le système d'équations $q_1(x_0, \cdots, x_4) = 0, q_2(x_0, \cdots, x_4) = 0$. Supposons que le groupe de Galois de $det(\lambda q_1 + \mu q_2)$ est le groupe S_5. Sous l'hypothèse de Schinzel et l'hypothèse de finitude des groupes de Tate-Shafarevich, le principe de Hasse vaut pour X.*

Théorème (Wittenberg, 2005) *Soit $X \subset \mathbf{P}^n_{\mathbf{Q}}$, $n \geq 5$ une intersection lisse de deux quadriques. Sous l'hypothèse de Schinzel et l'hypothèse de finitude des groupes de Tate-Shafarevich, le principe de Hasse vaut pour X.*

Au-delà de l'obstruction de Brauer-Manin

Il convient pour terminer de rappeler que Skorobogatov (1999) a donné un exemple de surface projective et lisse $X/\mathbf{Q}$ avec $X(A_{\mathbf{Q}})^{\mathrm{Br}(X)} \neq \emptyset$ et $X(\mathbf{Q}) = \emptyset$.

Ce sont des surfaces fibrées en courbes de genre 1, mais la fibration a des fibres multiples (ce sont des surfaces bielliptiques).

Equation :

$$y^2 = P(t)(x^2 + 1),\ z^2 = P(t)(x^2 + 2)$$

avec $P(t) = 3(t^4 - 54t^2 - 117t - 243)$.

Ce qui est ici employé, comme cela fut expliqué plus en détail dans des travaux ultérieurs de Harari et Skorobogatov, c'est l'existence de revêtements galoisiens finis non ramifiés de groupe de Galois non commutatif.