"Diophantine methods, lattices, and arithmetic theory of quadratic forms"
BIRS, Banff, Alberta, Canada, 14–18 November 2011

Sur l'équation $q(x, y, z) = P(t)$ en entiers

(Travail commun avec Fei XU, Beijing Capital Normal University)

Jean-Louis Colliot-Thélène

C.N.R.S., Université Paris-Sud, France

X une k-variété algébrique sur un corps de nombres k

Approximation forte hors de S

Soit $S \subset T$ avec T ensemble fini de places contenant les places archimédiennes et $\mathcal{X}/O_T$ un modèle de X/k sur l'anneau des T-entiers, puis pour chaque $v \in T \setminus S$, un ouvert $U_v \subset X(k_v)$. Dans toute telle situation, si l'ensemble

$$\prod_{v \in S} X(k_v) \times \prod_{v \in T \setminus S} U_v \times \prod_{v \notin T} \mathcal{X}(O_v)$$

est non vide, il contient l'image diagonale d'un point de $X(k)$.

Lorsque ceci vaut, on a un principe local-global pour les points S-entiers.

Pour $\mathcal{X}/O_S$ un modèle entier de X/k, si l'on a $\prod_{v \in S \cup \infty} X(k_v) \times \prod_{v \notin S} \mathcal{X}(O_v) \neq \emptyset$, alors $\mathcal{X}(O_S) \neq \emptyset$.

Sorites

• Si l'approximation forte hors de S vaut, elle vaut hors de tout S' contenant S.

• Si U ouvert non vide de X lisse et géométriquement intègre, si l'approximation forte hors de S vaut pour U, alors elle vaut pour X.

Cas classiques d'approximation forte

(1) $\mathbb{G}_a$: le théorème du reste chinois, S tout ensemble non vide de places

(2) $q(x_1, \ldots, x_n) = a$ avec $n \geq 4$, q isotrope en une place $v \in S$. (Eichler, Kneser)

(3) Groupe algébrique semisimple simplement connexe G/k sous une hypothèse forte de non compacité pour $\prod_{v \in S} G(k_v)$. (Kneser, Platonov)

L'approximation forte peut être en défaut.

Exemple de Borovoi et Rudnick (1995) :

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

soit encore

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

Solutions dans $\mathbb{Q}$

$$(x, y, z) = (-1/2, 1/2, 1) \qquad (x, y, z) = (1/3, 0, 1).$$

Donc solutions dans tous les $\mathbb{Z}_p$ avec $z = 1$.

Pas de solution dans $\mathbb{Z}$ pour $(y-x)(9x+7y) = 1-2z^2$
Soit (x, y, z) une solution. Un calcul 2-adique donne

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

Soit p premier. Si p divise $x-y$, alors p divise $2z^2 - 1$.
Ainsi p est impair et 2 est un carré mod. p
(deuxième loi complémentaire) $\Longrightarrow p \equiv \pm\, 1(8)$.
Donc $x - y \equiv \pm 1 \ (8)$.
Contradiction, $X(\mathbb{Z}) = \emptyset$.

De nombreux exemples de ce type, en particulier dans la famille à deux paramètres (Fei Xu et R. Schulze-Pillot) :

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

ont été interprétés (CT-Xu, 2005–2009) en terme de l'obstruction de Brauer-Manin (qui jusque là avait plutôt été considérée dans l'étude des points rationnels).

On utilise le groupe de Brauer des schémas et l'accouplement

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}$$

$$(\{M_v\}, A) \mapsto \sum_v \mathrm{inv}_v A(M_v),$$

qui est nul sur $X(k) \times \mathrm{Br}(X)$ (loi de réciprocité de la théorie du corps de classes). On note

$$X(\mathbb{A}_k)^{\mathrm{Br}(X)}$$

le noyau à gauche. On a donc $X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}(X)}$.

Approximation forte hors de S avec condition de Brauer-Manin. On suppose $X(\mathbb{A}_k) \neq \emptyset$.
Soit $S \subset T$ avec T ensemble fini de places contenant les places archimédiennes et $\mathcal{X}/O_T$ un modèle de X/k, puis pour chaque $v \in T \setminus S$, un ouvert $U_v \subset X(k_v)$. Dans toute telle situation, si l'ensemble

$$[\prod_{v \in S} X(k_v) \times \prod_{v \in T \setminus S} U_v \times \prod_{v \notin T} \mathcal{X}(O_v)]^{\mathrm{Br}(X)}$$

est non vide, il contient l'image diagonale d'un point de $X(k)$.

Sorites

• Si l'approximation forte hors de S avec condition de Brauer-Manin vaut pour S, elle vaut hors de tout S' avec $S \subset S'$.

• Si $X' \to X$ morphisme propre birationnel de variétés lisses, alors l'approximation forte avec condition de Brauer-Manin hors de S vaut pour X si et seulement si elle vaut pour X'.

Théorème (CT-Xu) *Soit $U \subset X$ un ouvert d'une k-variété lisse géométriquement intègre. Soit S un ensemble fini de places. On suppose $X(\mathbb{A}_k) \neq \emptyset$. Si $\mathrm{Br}(U)/\mathrm{Br}(X)$ est fini, et si l'approximation forte hors de S avec condition de Brauer-Manin vaut pour U, alors elle vaut pour X.*

[Utilise le lemme formel d'Harari.]

L'approximation forte hors de S avec condition de Brauer-Manin vaut pour :

X/k espace homogène d'un groupe algébrique G/k linéaire connexe, avec stabilisateurs géométriques connexes et hypothèse convenable de non compacité aux places de S.

CT et Xu 2005-2009 (G semisimple simplement connexe); Harari 2008 (G commutatif connexe); Demarche 2011 (groupes quelconques); Borovoi et Demarche (espaces homogènes, cas général).

Le cas intéressant le plus simple
Soit Y la k-variété définie par $q(x,y,z) = c$, avec q forme quadratique ternaire non dégénérée et $c \in k^{\times}$.
Soit $d = -c.\mathrm{det}(q)$.
Si $d \in k^{\times 2}$ alors $\mathrm{Br}(Y)/\mathrm{Br}(k) = 0$.
Si $d \notin k^{\times 2}$ alors $\mathrm{Br}(Y)/\mathrm{Br}(k) = \mathbb{Z}/2$, engendré par un élément $\xi \in \mathrm{Br}(Y)$ d'ordre 2, de la forme $(l(x,y,z), d)$ avec $l(x,y,z)$ fonction linéaire affine convenable.
Sur k corps de nombres, pour S fini contenant une place v avec q isotrope en v, on a l'approximation forte hors de S avec condition de Brauer-Manin – qui se réduit à la condition définie par ξ.

Calculs

• Sur k_v un corps local quelconque, avec $Y(k_v) \neq \emptyset$ et $d \notin k^{\times 2}$, ξ ne prend qu'une seule valeur sur $Y(k_v)$ si et seulement si v est une place réelle et q est anisotrope sur k_v.

• Sur k_v un corps p-adique non dyadique, q une forme non dégénérée sur o_v et $c \in o_v$, si $d = -c.\det(q)$ non carré, alors ξ prend deux valeurs distinctes sur les points $(x, y, z) \in Y(o_v)$ avec $(x, y, z) = 1$ (points primitifs) si et seulement si $v(c)$ est impaire.

Application.
Endliche Anzahl von Spinorausnahmen (M. Kneser, A. Weil)

Soit $q(x, y, z) \in \mathbb{Z}[x, y, z]$ indéfinie. Pour tout $c \in \mathbb{Z}$ non dans un ensemble fini $E = E(q) \subset \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, le principe local-global vaut pour les solutions entières de l'équation

$$q(x, y, z) = c.$$

Que dire sur les points entiers en dehors du cadre des espaces homogènes de groupes linéaires connexes ?

Penser à la situation analogue pour l'étude du principe local-global et l'approximation faible sur les points *rationnels*. Le cas des espaces homogènes de groupes algébriques linéaires connexes (avec stabilisateur connexe) a été beaucoup étudié (Eichler, Kneser, Harder, Chernousov, Sansuc, Borovoi). On a ensuite étudié l'extension à d'autres types de variétés, en particulier les variétés X avec une fibration $\pi : X \to \mathbb{A}^1_k$ dont la fibre générale est un tel espace homogène.

Soient k un corps, $q(x, y, z)$ une forme quadratique ternaire sur k, non dégénérée, et $P(t) \in k[t]$ non nul. Notons X/k la variété affine

$$q(x, y, z) = P(t).$$

Si $P(t)$ est séparable, X est lisse. Soit $U \subset X$ l'ouvert complémentaire de $x = y = z = 0$. C'est une variété lisse. Soit $\tilde{X} \to X$ une résolution des singularités de X, avec $U \subset \tilde{X}$.

Théorème principal de l'exposé (CT et Fei XU, 2011)

Pour k un corps de nombres et v_0 une place de k telle que q est isotrope sur k_{v_0}, l'approximation forte hors de $S = \{v_0\}$ avec condition de Brauer-Manin vaut pour tout ouvert Zariski V de X avec $U \subset V \subset \tilde{X}$.

$k = \mathbb{Q}$, S la place réelle.

L'approximation forte hors de S ne vaut pas en général pour $\tilde{X}$. Contre-exemple au principe local-global pour les solutions entières de

$$(y - x)(9x + 7y) + 2z^2 = (2t^2 - 1)^2.$$

L'approximation forte hors de S ne vaut pas en général pour U. Contre-exemple au principe local-global pour les solutions entières primitives $((x, y, z) = 1)$ de

$$x^2 - 2y^2 + 64z^2 = (2t^2 + 3)^2.$$

L'approximation forte hors de S vaut si le polynôme $P(t)$ n'est pas trop spécial.

Théorème :

Supposons de plus $P(t) \neq c.(r(t))^2$ avec $c \in k^\times$. Pour k un corps de nombres et v_0 une place de k telle que q est isotrope sur k_{v_0}, l'approximation forte hors de $S = \{v_0\}$ vaut pour tout ouvert Zariski V de X avec $U \subset V \subset \tilde{X}$.

Ceci est en fait un cas particulier du théorème principal, car on montre que l'hypothèse sur $p(t)$ implique

$$\mathrm{Br}(\tilde{X})/\mathrm{Br}(k) = \mathrm{Br}(U)/\mathrm{Br}(k) = 0,$$

il n'y a donc pas de conditions de Brauer-Manin à respecter.

Expliquons la démonstration du dernier théorème dans un cas particulier.

Théorème. *Soit* $q(x, y, z) \in \mathbb{Z}[x, y, z]$ *une forme quadratique ternaire entière indéfinie. Si* $P(t) \in \mathbb{Z}[t]$ *n'est pas égal à une constante fois un carré, le principe local-global vaut pour les solutions entières de l'équation* $q(x, y, z) = P(t)$*.*

Démonstration. Il y a un ensemble fini S de premiers tels que $q(x, y, z)$ représente tout élément de $\mathbb{Z}_p$ si $p \notin S$.
On se donne des solutions locales (x_p, y_p, z_p, t_p). On prend $t_0 \in \mathbb{Z}$ très proche de t_p pour $p \in S$. Il existe alors un entier $r > 0$ tel que, pour tout entier $m > 0$,

$$P(t_0 + (\prod_{p \in S} p)^r . m)$$

est représenté par $q(x, y, z)$ sur chacun des $\mathbb{Z}_p$.

Lemme. *Soit $P(t)$ un polynôme dans $\mathbb{Q}[t]$ qui n'est pas une constante fois un carré. L'ensemble des $P(m)$ pour $m \in \mathbb{N}$ parcourt une infinité de classes dans $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.* $\square$

On peut donc choisir $m = m_0$ de sorte que $P(t_0 + (\prod_{p \in S} p)^r.m_0)$ n'appartienne à aucune des classes exceptionnelles dans $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. L'équation

$$q(x, y, z) = P(t_0 + (\prod_{p \in S} p)^r.m_0)$$

qui a une solution sur chacun des $\mathbb{Z}_p$ et sur $\mathbb{R}$ a alors une solution $(x, y, z) \in \mathbb{Z}$. CQFD

Supposons maintenant $P(t) = c.(r(t))^2$, soit $P(t) = c.\prod_i P_i(t)^{e_i}$, avec les $P_i \in k[t]$ irréductibles et les e_i tous pairs.
Soit $d = -c.det(q)$. Soit $k_i = k[t]/(P_i)$.

• Si d carré dans k, alors $\mathrm{Br}(\tilde{X})/\mathrm{Br}(k) = \mathrm{Br}(U)/\mathrm{Br}(k) = 0$.

• Si d non carré dans k et il existe un i avec d non carré dans k_i, alors $\mathrm{Br}(\tilde{X})/\mathrm{Br}(k) = 0$ et $\mathrm{Br}(U)/\mathrm{Br}(k) = \mathbb{Z}/2$.

• Si d non carré dans k et carré dans chaque k_i, alors $\mathrm{Br}(\tilde{X})/\mathrm{Br}(k) = \mathrm{Br}(U)/\mathrm{Br}(k) = \mathbb{Z}/2$.

• De plus, pour tout $t_0 \in k$ avec $p(t_0) \neq 0$, la spécialisation $\mathrm{Br}(U)/\mathrm{Br}(k) \to \mathrm{Br}(U_{t_0})/\mathrm{Br}(k)$ est surjective.

Soit k corps de nombres. D'après une proposition vue au début, pour établir le théorème principal pour $\tilde{X}$, il suffit de le faire pour U. Soit $v_0 \in S$ avec q isotrope en v_0.
Considérons le cas $P(t) = c.(r(t))^2$ et d non carré dans k. On a alors $\xi \in \mathrm{Br}(U)$ d'ordre 2 engendrant $\mathrm{Br}(U)/\mathrm{Br}(k)$.
On suppose que ξ s'annule sur un point $\{M_v\}$ de

$$\prod_{v \in S} U(k_v) \times \prod_{v \in T \setminus S} U_v \times \prod_{v \notin T} \mathcal{U}(O_v)$$

où U_v est un ouvert dans $U(k_v)$:

$$\sum_v \xi(M_v) = 0.$$

Quitte à augmenter T, on peut supposer que q est non dégénérée sur o_T et que ξ s'annule sur $\mathcal{U}(O_v)$ pour $v \notin T$. Chaque M_v s'écrit (x_v, y_v, z_v, t_v). Par approximation forte sur k, on peut trouver t_0 entier en dehors de$T$, très proche de t_v pour $v \in T \setminus \{v_0\}$.
On peut alors remplacer chaque M_v pour $v \in T$ par un P_v de projection t_0 (en v_0, on utilise q isotrope), et qui de plus est très proche de M_v pour $v \in T \setminus \{v_0\}$. En tout tel v, on a
$\xi(M_v) = \xi(P_v)$.
Pour tout $v \notin T$, on choisit P_v quelconque dans $\mathcal{U}_{t_0}(o_v)$.

La restriction de $\xi \in \mathrm{Br}(U)$ engendre $\mathrm{Br}(U_{t_0})/\mathrm{Br}(k)$.
On a

$$\sum_v \xi(P_v) = \sum_v \xi(P_v) - \sum_v \xi(M_v) = \xi(P_{v_0}) - \xi(M_{v_0}) \in \mathbb{Z}/2.$$

Si d est un carré dans k_{v_0}, alors ξ est constant sur $U(k_{v_0})$.
Si d n'est pas un carré dans k_{v_0}, comme q est isotrope sur k_{v_0}, on a vu que ξ prend les deux valeurs $0, 1 \in \mathbb{Z}/2$ sur $U(k_{v_0})$. si $\xi(P_{v_0}) - \xi(M_{v_0}) \neq 0$, on change de P_{v_0}, ce qui est possible, et on assure

$$\sum_v \xi(P_v) = 0.$$

En appliquant le théorème d'approximation forte hors de S avec condition de Brauer-Manin sur les équations $q(x,y,z)=a$, on trouve un point de $U_{t_0}(k)$ dans la trace sur U_{t_0} de l'ouvert adélique donné au début. QED

Une question

Existe-t-il un ouvert de X qui est de la forme G/H avec G et H groupes linéaires connexes ?
Est-ce possible déjà sur un corps algébriquement clos ?

Que faire maintenant ?

- Pour $n \geq 4$

$$q(x_1, \ldots, x_n) = P(t)$$

avec q indéfinie en une place v_0. Facile. On a toujours approximation forte hors de $\{v_0\}$ pour le lieu lisse et pour une désingularisation.

Sans doute déjà dans des articles de Watson.

- L'équation

$$q(x, y) = P(t)$$

Très difficile si le degré de P est au moins 3. Il est déjà difficile de calculer $\mathrm{Br}(X)/\mathrm{Br}(k)$, cela requiert des considérations arithmétiques. Il n'est pas algébriquement clair que c'est un groupe fini.

Situation analogue

$$x^3 + y^3 + z^3 = n$$

sur $\mathbb{Z}$, étudiée par CT–Wittenberg 2010.
Pour n entier $n \neq \pm 4 \mod 9$, et $\mathcal{X}_n/\mathbb{Z}$ défini par

$$x^3 + y^3 + z^3 = n$$

puis $X_n = \mathcal{X}_n \times_{\mathbb{Z}} \mathbb{Q}$, on a

$$[\prod_p \mathcal{X}_n(\mathbb{Z}_p)]^{\mathrm{Br}(X_n)} \neq \emptyset.$$

- Étudier

$$\sum_{i=1}^{3} a_i(t) x_i^2 = P(t)$$

avec le produit $P(t).\prod_i a_i(t)$ sans facteur carré.
Devrait ne pas être beaucoup plus difficile que le théorème principal de l'exposé.
Plus généralement, étudier l'espace total d'une famille à un paramètre d'espaces homogènes.

Attention !

Pour des schémas quelconques sur $\mathbb{Z}$, les conditions de Brauer-Manin entières ne suffisent pas en général à garantir l'existence d'un point entier.
Exemple simple.
$\mathcal{X}/\mathbb{Z}$ défini dans $\mathbb{A}^4_{\mathbb{Z}}$ par

$$(16x^2 + 9y^2 - 3z^2).t = 1$$

Solution $\{M_p\} \in \prod_p \mathcal{X}(\mathbb{Z}_p)$ satisfaisant les conditions de Brauer-Manin, mais $\mathcal{X}(\mathbb{Z}) = \emptyset$.
Obstruction de Brauer-Manin étale entière (analogue de ce que fit Skorobogatov pour les points rationnels).