Reprinted from

Séminaire de Théorie des Nombres, Paris 1984–85

Edited by Catherine Goldstein

Progress in Mathematics, Volume 63

Birkhäuser
Boston · Basel · Stuttgart

SURFACES CUBIQUES DIAGONALES

J.-L. Colliot-Thélène

(d'après un travail en commun avec D. Kanevsky et J.-J. Sansuc)

Etant donnés des rationnels non nuls $a,b,c,d \in \mathbb{Q}^*$, peut-on décider si l'équation

$$(1) \qquad ax^3 + by^3 + cz^3 + dt^3 = 0$$

a une solution non triviale $(x,y,z,t) \in \mathbb{Q}^4$? En d'autres termes, peut-on décider si l'ensemble $V(\mathbb{Q})$ des points $\mathbb{Q}$-rationnels de la surface cubique lisse V définie dans l'espace projectif $\mathbb{P}^3_{\mathbb{Q}}$ par l'équation homogène (1) est non vide ?

L'objet de l'exposé, qui résume un travail en commun avec Kanevsky et Sansuc, à paraître ailleurs, est de décrire un algorithme conjectural permettant de décider si (1) a une solution. Plus précisément, cet algorithme calcule, de manière entièrement effective, l'obstruction de Brauer-Manin au principe de Hasse (telle que définie par Manin) pour les surfaces (1), et l'on conjecture qu'au moins pour ces surfaces cette obstruction est la seule. L'algorithme a permis à M. Vallino de tester cette conjecture sur l'ordinateur IBM 4341 de l'E.N.S. Ulm, et les résultats sont très encourageants.

Le plan de l'exposé est le suivant. Le paragraphe I contient l'historique du problème et rappelle la définition générale de l'obstruction de Brauer-Manin au principe de Hasse. Au paragraphe II, on donne la description complète de l'algorithme, dans tous ses détails pratiques, mais sans justification aucune des principaux énoncés : on se reportera à [5] pour les démonstrations, qui sont assez élaborées. Le paragraphe III donne des exemples d'utilisation de l'algorithme, les résultats des calculs sur ordinateur, et une application en dimension supérieure : si l'obstruction de Brauer-Manin au principe de Hasse est la seule pour les surfaces cubiques diagonales dans $\mathbb{P}^3_{\mathbb{Q}}$, alors le principe de Hasse vaut pour les hypersurfaces cubiques diagonales dans $\mathbb{P}^n_{\mathbb{Q}}$ $(n \geq 4)$.

§ 1. Historique.

Une condition évidente pour l'existence de solutions $\mathbb{Q}$-rationnelles de (1) (toujours supposées non triviales) est l'existence de solutions $\mathbb{Q}_p$-rationnelles pour tout complété p-adique de $\mathbb{Q}$ (le complété réel $\mathbb{R}$ ne pose pas de problème pour une surface cubique). Vérifier si ces conditions locales $V(\mathbb{Q}_p) \neq \emptyset$ sont satisfaites ne requiert, comme il est bien connu, qu'un nombre fini de vérifications.

En 1949, Mordell [10] conjecturait que les conditions locales suffisaient pour assurer l'existence d'un point $\mathbb{Q}$-rationnel sur une surface cubique, en d'autres termes que le principe de Hasse valait pour les surfaces cubiques. Dans le cas particulier des surfaces cubiques diagonales (1) telles que l'un des quotients ab/cd ou ac/bd ou ad/bc est un cube dans $\mathbb{Q}$, ceci fut établi en 1953 par Selmer [14] (une transformation algébrique simple permet de déduire le résultat du fait connu suivant : si K/k est une extension de corps de nombres de degré 3 - ou plus généralement de degré premier - tout élément de k qui est une norme de K/k partout localement l'est aussi globalement). Selmer vérifia aussi que toutes les surfaces (1) avec a,b,c,d entiers et $|abcd| \leq 500$ avaient un point $\mathbb{Q}$-rationnel dès que les conditions locales étaient vérifiées. Mais en 1962, Swinnerton-Dyer [15] réfuta la conjecture de Mordell pour les surfaces cubiques générales sur $\mathbb{Q}$ (voir aussi Mordell [11]) et en 1966, Cassels et Guy [3] donnèrent le premier exemple

$$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0 \tag{2}$$

de surface cubique diagonale (sur $\mathbb{Q}$) ne satisfaisant pas le principe de Hasse. Leur ordinateur leur avait en fait fourni une liste de quelques 250 équations du type (1) avec a,b,c,d entiers (petits), ayant des solutions partout localement et pas de solution rationnelle de petite hauteur (i.e. x,y,z,t entiers petits en valeur absolue). L'analyse de Cassels et Guy est courte, mais, de leur propre aveu, très sophistiquée. Ce n'est qu'en 1978 que Bremner [2] fournit un second exemple, lui aussi pris dans la liste originale,

$$x^3 + 4y^3 + 10z^3 + 25t^3 = 0 \tag{3}$$

de surface cubique diagonale sur $\mathbb{Q}$ contrevenant au principe de Hasse. Là encore, l'analyse est très élaborée, et nécessite la connaissance précise de l'arithmétique (groupes de classes, unités) de certains corps cubiques ou bicubiques. Aucune de ces analyses ne semble se prêter à une généralisation systématique qui mènerait à un algorithme au moins conjectural.

En 1970, Manin [8] proposa une interprétation générale de divers contre-exemples au principe de Hasse existant dans la littérature :

Soit V une variété projective, lisse et géométriquement intègre sur un corps de nombres k. Supposons $V(k_v) \neq \emptyset$ pour tout complété k_v de k. Si la condition :

$$(*) \qquad \forall \{P_v\} \in \prod_{v\in\Omega} V(k_v),\ \exists\, A \in \mathrm{Br}V,\ \sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) \neq 0 \in \mathbb{Q}/\mathbb{Z}$$

est vérifiée, alors l'ensemble $V(k)$ des points k-rationnels de V est vide.

Ici Ω désigne l'ensemble des places (finies ou infinies) de k, le groupe $\mathrm{Br}V$ est le groupe de Brauer-Grothendieck $H^2_{\acute{e}t}(V,\mathbb{G}_m)$ de V, et $\mathrm{inv}_v(A(P_v)) \in \mathbb{Q}/\mathbb{Z}$ est l'invariant local en v de la fibre $A(P_v) \in \mathrm{Br}k_v$ de A en P_v (la somme intervenant en (*) est finie pour des raisons de bonne réduction presque partout).

Si l'obstruction (*) vaut pour une k-variété V, nous dirons qu'il y a obstruction de Brauer-Manin au principe de Hasse pour V (cette obstruction est appelée de Manin dans [4] et [6]; elle est appelée de Brauer dans un article récent de Manin et Tsfasman), et nous dirons que l'obstruction de Brauer-Manin au principe de Hasse est vide pour V si la condition (*) n'est pas satisfaite. Etant donnée une <u>classe</u> C de k-variétés algébriques (projectives, lisses, géométriquement intègres) sur un corps de nombres k, il se pose alors les deux questions :

Question fondamentale : <u>L'obstruction de Brauer-Manin au principe de Hasse pour</u> C <u>est-elle la seule</u> ?

Question subsidiaire : <u>Etant donnée une</u> k-<u>variété</u> V <u>dans</u> C <u>qui possède des points rationnels partout localement, peut-on calculer effectivement l'obstruction</u> (*), <u>i.e. décider par un nombre fini d'opérations si elle est vide ou non</u> ?

Bien qu'il soit déraisonnable d'espérer que la question fondamentale ait une réponse affirmative pour la classe C de toutes les variétés algébriques, on ne connaît à ce jour aucun contre-exemple au principe de Hasse pour lequel (*) ne vaut pas - et pour la plupart des contre-exemples connus au principe de Hasse, on a pu les interpréter au moyen de l'obstruction de Brauer-Manin (voir [9], [4], [13]). Dans le cas des courbes de genre 1, la question est liée à la finitude du groupe de Tate-Shafarevitch (voir Manin [8] et [9], Théorème 41.24). Dans le cas des compactifiés lisses des espaces principaux homogènes de groupes algébriques linéaires connexes (sans facteur de type E_8), Sansuc [12] a montré que la question fondamentale a une réponse affirmative; mais sauf dans des cas très particuliers, la réponse à la question subsidiaire n'est pas claire : par exemple, étant donnée une extension finie de corps K/k, peut-on effectivement décider si un élément du corps de nombres k est une norme de l'extension K/k (voir cependant Bartels [1]) ? On espère que la question fondamentale a une réponse affirmative pour la classe C des surfaces rationnelles. On ne connaît pour l'instant ce résultat que pour les surfaces de Châtelet généralisées (voir [4], [13], [6]), qui sont les surfaces rationnelles "non triviales" les plus simples. Dans ce cas, la question subsidiaire a une réponse affirmative facile. Par contre la question fondamentale et aussi la subsidiaire sont ouvertes déjà pour les intersections lisses de deux quadriques dans $\mathbb{P}^4$ et pour les surfaces cubiques lisses dans $\mathbb{P}^3$.

A la fin de son livre [9], Manin fait une tentative pour interpréter le contre-exemple (2) de Cassels-Guy en termes de l'obstruction de Brauer-Manin, i.e. pour établir (*), ou du moins une condition voisine, mais le calcul est peu convaincant et surtout ne semble pas s'étendre à d'autres exemples. L'algorithme qui suit répond entièrement à la question subsidiaire pour la classe C des surfaces cubiques diagonales sur $\mathbb{Q}$ - ce qui permet alors de tester sur ordinateur la question fondamentale pour cette même classe.

§ II. L'algorithme.

Etant donnée une surface cubique diagonale $V \subset \mathbb{P}^3_{\mathbb{Q}}$ définie par une équation

$$(1) \qquad ax^3 + by^3 + cz^3 + dt^3 = 0,$$

l'algorithme suivant conclut : <u>soit</u> $V(\mathbb{Q})$ est vide, <u>soit</u> $V(\mathbb{Q}_p)$ est non vide pour tout premier p et l'obstruction de Brauer-Manin au principe de Hasse pour V est vide (ce qui est bien sûr le cas si $V(\mathbb{Q}) \neq \emptyset$).

a) Par multiplication des coordonnées et de l'équation par des rationnels, on peut supposer que les coefficients a,b,c,d sont entiers naturels et que pour chaque nombre premier p, l'ensemble des valuations $(v_p(a),v_p(b),v_p(c),v_p(d))$ est, à permutation près, de l'un des types $(0,0,0,0),(0,0,0,1),(0,0,0,2),(0,0,1,1),(0,0,1,2)$ (il existe d'ailleurs une unique équation réduite de ce type : elle minimise le produit $abcd$ parmi toutes les équations (1) à coefficients entiers équivalentes).

b) Si l'un des quotients a/b, a/c, a/d, b/c, b/d, c/d est un cube dans $\mathbb{Q}$, alors clairement $V(\mathbb{Q}) \neq \emptyset$: STOP. Sinon,

c) Calculer si $V(\mathbb{Q}_p)$ est vide pour un certain premier p. En utilisant le lemme de Hensel, on trouve facilement :

Pour $p \equiv 2\ (3)$, l'équation (1) a toujours une solution dans $\mathbb{Q}_p$. Pour $p \equiv 1\ (3)$, et (1) sous forme réduite, l'équation (1) a une solution dans $\mathbb{Q}_p$ sauf si, à permutation près, les coefficients sont

(a_1,b_1,pc_1,pd_1) avec $a_1,\dots,d_1$ de p-valuation nulle et a_1/b_1 et c_1/d_1 non cubes dans le corps fini $\mathbb{F}_p$,

ou

(a_1,b_1,pc_1,p^2d_1) avec $a_1,\dots,d_1$ de p-valuation nulle et a_1/b_1 non cube dans $\mathbb{F}_p$.

Enfin, pour $p=3$, et (1) sous forme réduite, l'équation (1) a une solution dans $\mathbb{Q}_3$, sauf si, à permutation près, les coefficients sont $(a_1,b_1,c_1,9d_1)$, avec $a_1,\dots,d_1$ unités 3-adiques et (a_1,b_1,c_1) égal à permutation près au triplet $(1,2,4)$ modulo 9.

N.B. Une unité $u \in \mathbb{Z}_p^*$ est un cube si et seulement si $p \equiv 2\ (3)$, ou $p \equiv 1\ (3)$ et u est un cube modulo p, ou $p=3$ et $u \equiv \pm 1 (9)$.

Si $V(\mathbb{Q}_p) = \emptyset$ pour un certain p, alors $V(\mathbb{Q}) = \emptyset$: STOP.

Sinon, i.e. si $V(\mathbb{Q}_p)$ est non vide pour tout p,

d) Si l'un des quotients ab/cd, ac/bd, ad/bc est un cube dans $\mathbb{Q}$, alors $V(\mathbb{Q}) \neq \emptyset$ (Selmer [14]) : STOP. Sinon,

e) Soit S l'ensemble des nombres premiers qui divisent $3abcd$ (pour (1) sous la forme réduite). S'il existe p dans S tel qu'aucun des quotients ad/bc, ab/cd, ac/bd ne soit un cube dans $\mathbb{Q}_p$, STOP ! En effet, sous cette hypothèse, on a alors le :

Théorème. L'obstruction de Brauer-Manin au principe de Hasse pour V est vide.

Sinon, i.e. si pour chaque p dans S, l'un au moins des 3 quotients ci-dessus est un cube dans $\mathbb{Q}_p$,

f) Par multiplication de l'équation réduite et des coordonnées par des rationnels dont tous les facteurs premiers divisent $abcd$, et par permutation éventuelle de (a,b,c,d), ramener l'équation (1) à une équation de la forme :

$$x^3 + \lambda y^3 + \mu z^3 + \lambda \mu \nu t^3 = 0 , \tag{4}$$

avec λ, μ, ν entiers sans facteurs cubiques, et ν cube dans $\mathbb{Q}_3$ (ce qui est possible car 3 est dans S). Un calcul simple montre qu'alors :

(5) Pour tout premier p, l'un au moins de $\lambda, \nu, \lambda/\nu, \lambda\nu$ est un cube dans $\mathbb{Q}_p$.

Choisissons α et γ dans une clôture algébrique fixe $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, tels que $\alpha^3 = \lambda$ et $\gamma^3 = \nu$, puis définissons β et δ dans $\overline{\mathbb{Q}}$ via $\beta = \alpha\gamma$ et $\delta = \alpha/\gamma$ (donc $\beta^3 = \lambda\nu$ et $\delta^3 = \lambda/\nu$).

Choisissons aussi $\theta \in \overline{\mathbb{Q}}$ une racine primitive cubique de 1, et soit $k = \mathbb{Q}(\theta)$ l'extension quadratique qu'elle définit. Soit $K = k(\alpha, \gamma)$. Les hypothèses faites après b) et d) montrent que K/k est une extension (de corps) de degré 9, galoisienne de groupe $G \simeq \mathbb{Z}/3 \times \mathbb{Z}/3$, et (5) implique

(6) Pour toute place v de k, le groupe de décomposition $G_v \subset G$ associé est cyclique.

On a le diagramme de corps :

$$\begin{tikzcd}
 & & & K \arrow[dlll, dash, "\langle t\rangle"'] \arrow[dl, dash, "\langle r\rangle"'] \arrow[dr, dash, "\langle q\rangle"] \arrow[drrr, dash, "\langle s\rangle"] & & & \\
k(\gamma) \arrow[drrr, dash] & & k(\delta) \arrow[dr, dash] & & k(\beta) \arrow[dl, dash] & & k(\alpha) \arrow[dlll, dash] \\
 & & & k = \mathbb{Q}(\theta) \arrow[d, dash] & & & \\
 & & & \mathbb{Q} & & &
\end{tikzcd}$$

où $s,t,r,q \in G = \mathrm{Gal}(K/k)$ sont définis par ${}^s\alpha = \alpha$ et ${}^s\gamma = \theta\gamma$, puis ${}^t\alpha = \theta\alpha$ et ${}^t\gamma = \gamma$, enfin $r = st$ et $q = st^2$.

g) On a alors la

Proposition. Sous les hypothèses précédentes, il existe $\varepsilon_\beta \in \mathbb{Q}(\beta)$ et $\varepsilon_\delta \in \mathbb{Q}(\delta)$ tels que :

$$N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\varepsilon_\beta) \cdot N_{\mathbb{Q}(\delta)/\mathbb{Q}}(\varepsilon_\delta) = \mu,$$

où N désigne la norme. On peut en fait choisir $\varepsilon_\beta = 1$ ou $\varepsilon_\delta = 1$.

L'étape suivante de l'algorithme consiste à chercher explicitement un couple $(\varepsilon_\beta, \varepsilon_\delta)$ comme ci-dessus. Il s'agit là d'un problème fini (voir Bartels [1]). En pratique, on remarque que tout élément de $\mathbb{Q}(\beta)$ s'écrit comme un quotient $(m+n\beta)/(p+q\beta)$ avec m et n entiers, et que la norme de $(m+n\beta)$ est simplement $m^3 + \lambda\nu n^3$. De même dans $\mathbb{Q}(\delta)$. On fait donc des tables de produits et de quotients de rationnels de la forme $m^3 + \lambda\nu n^3$ et $m^3 + (\lambda/\nu)n^3$, avec m et n entiers petits en valeur absolue, et l'on cherche μ dans ces tables. C'est là qu'il y a avantage à ne pas se restreindre au cas $\varepsilon_\beta = 1$ ou $\varepsilon_\delta = 1$.

h) Une fois un couple $(\varepsilon_\beta, \varepsilon_\delta)$ déterminé, on définit l'ensemble fini S_1 des places v de $k = \mathbb{Q}(\theta)$, non archimédiennes et non 3-adiques, et telles que : soit v est au-dessus d'un p premier appartenant à S, soit il existe une place w de $k(\beta)$ au-dessus de v avec $w(\varepsilon_\beta) \neq 0$, soit il existe une place w de $k(\delta)$ au-dessus de v avec $w(\varepsilon_\delta) \neq 0$. Dans la suite, pour chaque place v de $k = \mathbb{Q}(\theta)$, on utilise le symbole de reste normique (pour l'exposant 3) qui à un couple d'éléments ξ, η de k_v^* associe un élément $[\xi,\eta]_v \in \mathbb{Z}/3$. On trouvera plus bas le formulaire bien connu permettant de calculer ces symboles dans le cas modéré (v finie non 3-adique) qui suffit ici.

Pour chaque place $v \in S_1$, on calcule alors un élément $i_v \in \mathbb{Z}/3$ à l'aide du tableau suivant :

Cube dans $\mathbb{Q}_p$	ν	λ/ν	$\lambda\nu$	λ
i_v	0	$[{}^q\varepsilon_\delta/\varepsilon_\delta, \nu]_v$	$[\theta^2 \cdot \varepsilon_\beta/{}^r\varepsilon_\beta, \nu]_v$	$[\theta,\nu]_v$

Ce tableau s'utilise de la façon suivante. On note p le premier de $\mathbb{Q}$ au-dessus duquel est v. D'après (5), l'un au moins des 4 nombres

ν, λ/ν, $\lambda\nu$, λ est un cube dans $\mathbb{Q}_p$. On choisit l'un de ceux qui est un cube, et la valeur de i_v est alors donnée par la seconde ligne du tableau. Les valeurs correspondant à λ/ν ou $\lambda\nu$ cubes requièrent une explication. Supposons que λ/ν est un cube dans $\mathbb{Q}_p$. On dispose alors de trois plongements $\sigma : k(\delta) \longrightarrow k_v$ qui étendent le plongement naturel de k dans k_v. En utilisant le fait que l'équation (4) a des solutions dans $\mathbb{Q}_p$ et en utilisant l'égalité $N_{k(\beta)/k}(\varepsilon_\beta) \cdot N_{k(\delta)/k}(\varepsilon_\delta) = \mu$ (voir g), et les propriétés usuelles du symbole de reste normique, on montre que la valeur de $[\sigma({}^q\varepsilon_\delta/\varepsilon_\delta),\nu]_v$ ne dépend pas du choix du plongement σ comme ci-dessus : c'est cette valeur commune qu'on note, de façon abusive, $[{}^q\varepsilon_\delta/\varepsilon_\delta,\nu]_v$. La situation lorsque $\lambda\nu$ est un cube dans $\mathbb{Q}_p$ est entièrement analogue.

L'algorithme se conclut alors avec le théorème suivant :

Théorème. Avec les hypothèses et notations précédentes, l'obstruction de Brauer-Manin au principe de Hasse pour V est vide si et seulement si

$$I = \sum_{v \in S_1} i_v = 0 \in \mathbb{Z}/3 .$$

En particulier, si $I \neq 0$, alors $V(\mathbb{Q}) = \emptyset$ et V est un contre-exemple au principe de Hasse.

i) Appendice : formulaire pour le symbole de restes normiques.

Les conventions de signe variant dans la littérature, et le théorème ci-dessus faisant intervenir une somme, il est important de fixer une convention. Soit v une place finie non 3-adique de $k = \mathbb{Q}(\theta)$ (seules ces places interviennent ci-dessus). Le symbole de reste normique pour l'exposant 3 est une application bimultiplicative et alternée de $k_v^* \times k_v^*$ dans $\mathbb{Z}/3$, qui s'annule sur les couples (u_1,u_2) formés d'unités locales. Il suffit donc de connaître sa valeur sur les couples (u,p) où u est une unité du corps local k_v et où p est le premier de $\mathbb{Q}$ au-dessous de v (c'est une uniformisante de k_v). Notons θ_v l'image de $\theta \in k \subset k_v$, vue comme unité de k_v, dans le corps résiduel de k_v, qui est soit $\mathbb{F}_p$ si $p \equiv 1$ (3), soit $\mathbb{F}_p(\theta_v)$ $(\simeq \mathbb{F}_{p^2})$ si $p \equiv 2$ (3). La valeur de $[u,p]_v$ est donnée par la classe modulo 3 de tout entier m tel que

$$u^{(p-1)/3} \equiv \theta_v^m \in \mathbb{F}_p \qquad \text{si } p \equiv 1(3)$$

$$u^{(p^2-1)/3} \equiv \theta_v^m \in \mathbb{F}_p(\theta_v) \qquad \text{si } p \equiv 2(3).$$

§ III. Mise en oeuvre et applications.

III.1. L'exemple de Cassels et Guy.

L'équation $5x^3+9y^3+10z^3+12t^3=0$ survit aux étapes a) à e) de l'algorithme. On la ramène alors à l'équation du type (4) :

$$x^3+15y^3+30z^3+15\times 30\times 10\,t^3=0\ ,$$

soit $\lambda=15$, $\mu=30$, $\nu=10$. On a $N_{\mathbb{Q}(\beta)/\mathbb{Q}}(m+n\beta)=m^3+150n^3$, ce qui donne pour $(m,n)=(5,0)$, resp. $(0,1)$, resp. $(-5,1)$, les valeurs 125, resp. 150, resp. 25, si bien que l'on a :

$$N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta(\beta-5)/5)=30=\mu.$$

On peut donc prendre $\varepsilon_\beta=\beta(\beta-5)/5$ et $\varepsilon_\delta=1$. Les seules places $v\in S_1$ sont les places v_2 et v_5 de $k=\mathbb{Q}(\theta)$ situées au-dessus des premiers 2 et 5 (inertes dans $\mathbb{Q}(\theta)$). Comme $\lambda=15$ est un cube dans $\mathbb{Q}_2$, la valeur de i_{v_2} est donnée (voir le tableau) par :

$$i_{v_2}=[\theta,10]_{v_2}=[\theta,2]_{v_2}=1\ (\mathrm{mod.}\ 3)$$

(cas trivial d'application du formulaire). Par ailleurs, $\lambda/\nu=3/2$ est un cube dans $\mathbb{Q}_5$, et $\varepsilon_\delta=1$: le tableau donne alors trivialement la valeur $i_{v_5}=0$. Ainsi $I=i_{v_2}+i_{v_5}=1\neq 0$, et (2) n'a pas de solution non triviale dans $\mathbb{Q}$.

III.2. L'exemple de Bremner généralisé.

On considère l'équation

$$x^3+p^2y^3+pqz^3+q^2t^3=0 \tag{7}$$

avec p et q premiers, $p\equiv 2(9)$ et $q\equiv 5(9)$. Cette équation généralise clairement l'équation (3), et l'on vérifie aisément qu'elle a des solutions dans tous les complétés de $\mathbb{Q}$ (voir § II, c). On vérifie facilement que (7) survit aux étapes a) à e) de l'algorithme. On se ramène à l'équation de type (4) :

$$x^3 + p\,y^3 + p^2q\,z^3 + (p \times p^2q \times pq)\,t^3 = 0\,,$$

soit $\lambda = p$, $\mu = p^2q$ et $\nu = pq$. On a en particulier

$$\mu = \lambda\nu = \beta^3 = N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta),$$

ce qui permet de choisir $\varepsilon_\beta = \beta$ et $\varepsilon_\delta = 1$ au point g) de l'algorithme. Les seules places dans S_1 sont les places v_p et v_q de $\mathbb{Q}(\theta)$ au-dessus des premiers inertes p et q. Dans $\mathbb{Q}_p$, le rationnel $\lambda/\nu = 1/q$ devient un cube et comme $\varepsilon_\delta = 1$, le tableau donne $i_{v_p} = 0$. Dans $\mathbb{Q}_q$, c'est $\lambda = p$ qui est un cube. On a donc

$$i_{v_q} = [\theta,pq]_{v_q} = [\theta,q]_{v_q} \equiv (q^2-1)/3 \equiv 2 \ (3)$$

(encore une application simple du formulaire en i), et de $q \equiv 5(9)$). Ainsi $I = i_{v_p} + i_{v_q} = 2 \neq 0$, et (7) n'a pas de solution non triviale dans $\mathbb{Q}$: on a ainsi produit une série infinie de contre-exemples au principe de Hasse.

III.3. Résultats du calcul sur ordinateur (M. Vallino).

On a considéré toutes les équations

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

avec a,b,c,d entiers naturels strictement plus petits que 100. Chaque équation a été réduite (II.a), sauf lorsque la réduction amenait l'un des coefficients à être supérieur ou égal à 100. On a éliminé les équations qui n'avaient pas de solution dans un complété $\mathbb{Q}_p$ (voir II.c) et aussi celles considérées en II.b, qui ont clairement un point rationnel. Pour chacune des équations restantes, on a cherché des solutions avec x,y,z,t entiers relatifs et

$$\sup(|x|,|y|,|z|,|t|) \leq 8000.$$

Pour chacune des équations qui étaient restées sans solution, l'ordinateur a vérifié via l'algorithme décrit au § II (en fait une version antérieure, légèrement plus compliquée) que l'obstruction de Brauer-Manin était non vide.

En d'autres termes : Dans le domaine $\sup(|a|,|b|,|c|,|d|) < 100$, l'obstruction de Brauer au principe de Hasse pour les surfaces cubiques d'équation

$$ax^3 + by^3 + cz^3 + dt^3 = 0 \qquad (a,b,c,d \text{ entiers})$$

est la seule.

On trouvera ci-après la table établie par M. Vallino donnant tous les contre-exemples au principe de Hasse dans le domaine considéré (les calculs ont été faits le 13 mars 1985 au Centre de Calcul de l'E.N.S. Ulm sur IBM 4341). Plus précisément, pour décider si une équation (à coefficients entiers naturels) dans ce domaine a un point rationnel, on détermine d'abord si elle a des solutions dans tous les $\mathbb{Q}_p$. Si oui, on la réduit - mais pas exactement suivant la procédure indiquée au § II, a), ce qui amènerait certains coefficients à dépasser 100, mais seulement de façon à minimiser $abcd$ tout en laissant chaque coefficient < 100 (il y a ainsi des surfaces équivalentes dans la table, mais l'équivalence passe par une équation dont un des coefficients dépasse 100 - e.g. (2,4,10,25) et (4,5,10,25)). Si l'équation obtenue (avec $a < b < c < d$) est dans la table, c'est que l'obstruction de Brauer-Manin est non vide et qu'il n'y a donc pas de solution non triviale dans $\mathbb{Q}$; sinon, c'est que l'ordinateur a trouvé une solution non triviale dans $\mathbb{Q}$ (avec $\sup(|x|,|y|,|z|,|t|) \leq 8000$).

N.B. Pour se convaincre de l'efficacité de l'algorithme du § II, l'appliquer - à la main - à une équation prise au hasard dans la table (ce sont a priori les plus délicates - voir par exemple l'énoncé III.4). En fait, le temps d'ordinateur requis pour effectuer l'algorithme sur une équation donnée est très petit (~ 1s), sans commune mesure avec le temps nécessaire pour trouver une solution dans $\mathbb{Q}$.

Table : Contre-exemples au principe de Hasse

a	b	c	d
1	2	30	75
1	4	10	25
1	4	15	90
1	4	30	45
1	4	30	75
1	5	12	30
1	6	25	90
1	6	34	51
1	10	20	50
1	10	34	85
1	10	36	75
1	12	25	30
1	12	51	68
1	15	51	85
1	18	25	30
1	20	68	85
1	21	36	98
1	30	50	60
2	3	33	44
2	4	10	25
2	4	15	75
2	4	66	99
2	5	36	75
2	6	51	68
2	9	10	75
2	9	44	99
2	10	68	85
2	12	17	51
2	12	22	33
2	12	25	90
2	12	58	87
2	17	20	85
2	22	25	55
2	25	30	36
2	30	33	55
2	44	50	55
2	51	60	85
2	55	60	66
2	55	66	75
2	55	90	99
2	57	60	95
3	4	10	15
3	4	25	90
3	4	46	69
3	5	10	36
3	6	10	25
3	6	44	99
3	9	34	68
3	11	18	44
3	17	18	34
3	17	45	85
3	18	49	84
3	20	50	90
3	23	36	46
3	25	30	36
3	34	85	90
3	36	41	82
3	38	90	95
3	44	55	90
3	50	55	66
4	5	10	25
4	5	75	90
4	6	17	51
4	6	25	30
4	6	25	45
4	6	69	92
4	10	11	55
4	10	15	75
4	10	17	85
4	10	18	75
4	11	50	55
4	12	34	51
4	15	18	25
4	15	25	30
4	20	22	55
4	20	34	85
4	25	44	55
4	30	33	55
4	60	75	90
5	6	12	25
5	9	10	12
5	9	50	60
5	17	34	50
5	17	51	75
5	22	25	44
5	25	34	68
5	25	36	60
5	25	36	90
5	30	46	69
5	60	69	92
6	9	11	44
6	9	17	34
6	9	25	30
6	10	12	25
6	11	55	90
6	12	22	99
6	15	25	36
6	20	51	85
6	20	55	66
6	25	36	90
6	25	55	66
6	29	36	58
6	30	55	99
6	35	50	84
6	44	45	55
6	68	85	90
9	10	15	50
9	10	25	60
9	12	23	46
9	12	41	82
9	15	17	85
9	18	33	44
9	18	34	51
9	28	70	75
9	30	34	85
9	30	44	55
9	36	46	69
9	36	51	68
9	45	51	85
9	50	60	90
9	60	68	85
10	11	22	25
10	11	66	75
10	12	25	45
10	12	51	85
10	12	55	99
10	15	51	68
10	17	25	34
10	17	25	68
10	22	25	44
10	22	75	99
10	23	25	92
10	23	60	69
10	25	29	58
10	25	33	66
10	25	46	92
10	25	63	84
10	30	69	92
10	33	44	75
10	33	50	99
10	34	51	60
10	36	51	85
10	49	60	63
10	52	75	78
10	69	75	92
11	18	30	55
11	18	36	66
11	30	33	50
11	30	44	75
11	36	55	90
11	44	75	90
11	49	66	84
11	50	66	75
11	50	90	99
12	15	25	90
12	17	30	85
12	18	29	58
12	30	49	70
12	33	50	55
12	33	55	90
12	34	60	85
12	45	68	85
12	51	85	90
14	18	35	60
14	18	49	84
15	17	25	51
15	17	68	90
15	18	44	55
15	20	21	98
15	21	28	50
15	21	90	98
15	23	46	90
15	34	68	75
15	36	68	85
15	45	46	92
15	46	75	92
17	18	36	51
17	20	50	85
17	30	34	75
17	30	36	85
17	30	45	68
17	34	75	90
18	22	33	36
18	22	55	75
18	33	55	90
18	35	45	84
18	36	58	87
18	36	69	92
20	22	25	55
20	22	66	75
20	23	25	46
20	23	30	69
20	25	41	82
20	29	50	58
20	33	50	66
20	36	55	66
20	41	50	82
20	44	50	55
20	46	60	69
20	46	69	75
20	47	50	94
20	51	68	75
20	55	77	98
22	25	50	55
22	25	60	66
22	30	44	75
22	33	50	60
22	33	69	92
22	33	75	90
23	30	45	46
23	30	46	75
23	30	75	92
23	66	92	99
25	26	39	60
25	30	33	44
25	30	34	51
25	30	44	66
25	30	46	69
25	30	58	87
25	30	66	99
25	34	50	85
25	42	45	98
25	44	45	66
25	44	60	66
25	44	66	75
25	44	90	99
25	46	60	69
25	50	66	99
25	51	60	68
25	51	68	90
25	51	75	85
25	55	60	66
28	30	49	75
29	30	58	75
30	33	44	50
30	34	68	75
30	36	55	99
30	41	75	82
30	47	75	94
30	49	70	75
30	50	69	92
33	34	44	51
34	36	60	85
34	36	75	85
34	44	55	85
34	45	68	75
34	50	51	60
34	66	68	99
35	36	50	63
36	38	60	95
36	44	55	75
36	51	85	90
36	57	90	95
36	77	98	99
44	50	60	99
44	51	66	68
44	66	75	90
44	75	90	99
45	46	69	90
45	47	60	94
45	49	60	84
45	51	68	90
46	50	60	69
47	66	94	99
50	55	60	99
50	60	66	99
58	69	87	92
58	75	87	90
68	75	85	90

III.4. Un cas simple où l'obstruction de Brauer est vide.

Soit $V \subset \mathbb{P}^3_{\mathbb{Q}}$ une surface cubique diagonale, d'équation

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

avec a,b,c,d entier non nuls, sans facteur cubique. Supposons $V(\mathbb{Q}_p) \neq \emptyset$ pour tout premier p. Alors, s'il existe un premier p qui divise l'un des coefficients (nécessairement avec l'exposant 1 ou 2) mais ne divise aucun des autres coefficients, l'obstruction de Brauer-Manin au principe de Hasse pour V est vide.

De fait, soit l'algorithme s'arrête avant le point *e*) et on sait qu'il y a un point rationnel sur $\mathbb{Q}$, soit le théorème du point *e*) s'applique : aucun quotient ab/cd, ad/bc, ac/bd, dont la valuation p-adique n'est pas divisible par 3, ne saurait être un cube dans $\mathbb{Q}_p$.

On est bien tenté de conjecturer que, sous les conditions ci-dessus, $V(\mathbb{Q})$ est non vide, conjecture vérifiée par l'ordinateur dans le domaine indiqué en III.3.

III.5. Hypersurfaces cubiques diagonales.

Proposition. Si l'obstruction de Brauer-Manin au principe de Hasse pour les surfaces cubiques diagonales $V \subset \mathbb{P}^3_{\mathbb{Q}}$ est la seule, alors les hypersurfaces cubiques diagonales $X \subset \mathbb{P}^n_{\mathbb{Q}}$ $(n \geq 4)$ satisfont le principe de Hasse.

Démonstration. Soit $\sum_{i=0}^{n} a_i x_i^3 = 0$, avec a_i entiers non nuls l'équation d'une telle hypersurface X, dont on suppose qu'elle a des points rationnels dans tous les complétés de $\mathbb{Q}$. Soit S l'ensemble fini des premiers p qui divisent $3 \prod_{i=0}^{n} a_i$. Pour chaque p dans S, choisissons un point $((x_{i,p})_{i=0,\ldots,n})$ de $X(\mathbb{Q}_p)$, avec chaque $x_{i,p}$ entier p-adique et avec $\sum_{i \geq 3} a_i x_{i,p}^3 \neq 0$ (ce qui est possible). Soit alors q un nombre premier congru à 2 modulo 3 et non dans S. On peut trouver $((x_{i,q})_{i=3,\ldots,n})$ dans $\mathbb{Z}^{n-2}$ tel que $\sum_{i=3}^{n} a_i x_{i,q}^3$ soit divisible par q mais non par q^2. En utilisant le théorème des restes chinois, on peut alors trouver $(\alpha_i)_{i \geq 3}$ dans $\mathbb{Z}^{n-2}$ tel que $d = \sum_{i \geq 3} a_i \alpha_i^3$ soit non nul et satisfasse :

i) $(\sum_{i\geq 3} a_i x_{i,p}^3)/d$ est un cube dans $\mathbb{Q}_p$ $(p \in S)$

ii) q divise d mais q^2 ne divise pas d.

Considérons alors la surface cubique diagonale $V \subset \mathbb{P}^3_{\mathbb{Q}}$ d'équation :

$$\sum_{i=0}^{2} a_i x_i^3 + dt^3 = 0.$$

Cette surface cubique a des points dans tous les complétés $\mathbb{Q}_p$: pour $p \in S$, cela résulte de i) ci-dessus, et pour $p \notin S$, cela résulte simplement de ce que la courbe de genre 1 définie par $\sum_{i=0}^{2} a_i x_i^3 = 0$ a bonne réduction en p, donc a des points dans $\mathbb{Q}_p$. Par ailleurs, le premier $q \notin S$ ne divise aucun des a_i, mais il divise d avec l'exposant 1, d'après ii). Il ne reste plus qu'à appliquer l'énoncé de III.4.

<u>Remarque</u>. On notera la perversité de l'argument, qui consiste à trouver une surface cubique $V \subset X$ par sections linéaires, de telle sorte que $V(\mathbb{Q}_p)$ soit non vide pour tout p, et pour laquelle l'obstruction de Brauer-Manin est vide - mais sans que cela soit dû, comme dans les réductions analogues effectuées dans [6], à la trivialité $(\mathrm{Br}V = \mathrm{Br}\mathbb{Q})$ du groupe de Brauer de la section linéaire V.

On trouvera dans l'exposé de Kanevsky à Besançon [7] d'autres énoncés reposant sur la conjecture que l'obstruction de Brauer-Manin au principe de Hasse est la seule pour certaines classes de variétés. On peut en fait montrer que le groupe de Brauer d'une hypersurface cubique lisse $X \subset \mathbb{P}^n_k$ $(n \geq 4)$ est trivial, si bien que si l'obstruction de Brauer-Manin au principe de Hasse est la seule pour une classe de variétés contenant les hypersurfaces cubiques lisses, certainement le principe de Hasse vaut pour elles ! L'intérêt d'une proposition comme celle ci-dessus est qu'elle ramène à un problème sur les <u>surfaces</u> cubiques, dont la géométrie semble plus prometteuse.

BIBLIOGRAPHIE

[1] H.-J. Bartels.- Ueber Normen algebraischer Zahlen, Math. Ann. 251, 191-212 (1980).

[2] A. Bremner.- Some cubic surfaces with no rational points, Math. Proc. Camb. Phil. Soc. 84, 219-225 (1978).

[3] J.W.S. Cassels and M.J.T. Guy.- On the Hasse principle for cubic surfaces, Mathematika 13, 111-120 (1966).

[4] J.-L. Colliot-Thélène, D. Coray et J.-J. Sansuc.- Descente et principe de Hasse pour certaines variétés rationnelles, J. reine angew. Math. 320, 150-191 (1980).

[5] J.-L. Colliot-Thélène, D. Kanevsky et J.-J. Sansuc.- Arithmétique des surfaces cubiques diagonales (prépublication).

[6] J.-L. Colliot-Thélène, J.-J. Sansuc and Sir Peter Swinnerton-Dyer.- Intersections of two quadrics and Châtelet surfaces (prépublication, voir C.R. Acad. Sc. Paris, 298, Série I, 377-380 (1984)).

[7] D. Kanevsky.- Exposé aux journées arithmétiques de Besançon (juin 1985).

[8] Yu.I. Manin.- Le groupe de Brauer-Grothendieck en géométrie diophantienne, Actes du Congrès Intern. Math. Nice 1, 401-411 (1970).

[9] Yu.I. Manin.- Formes cubiques, Algèbre, Géométrie, Arithmétique, Nauka, Moscou (1972), trad. ang. North-Holland, Amsterdam (1974).

[10] L.J. Mordell.- Rational points on cubic surfaces, Publ. Math. Debrecen 1, 1-6 (1949).

[11] L.J. Mordell.- On the conjectures for rational points on a cubic surface, Journal London Math. Soc. 40, 149-158 (1965).

[12] 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).

[13] J.-J. Sansuc.- Descente et principe de Hasse pour certaines variétés rationnelles, Séminaire de Théorie des Nombres, Paris 1980-81, Progress in Math. 22, Birkhäuser (1982).

[14] E.S. Selmer.- Sufficient congruence conditions for the existence of rational points on certain cubic surfaces, Math. Scand. 1, 113-119 (1953).

[15] H.P.F. Swinnerton-Dyer.- Two special cubic surfaces, Mathematika 9, 54-56 (1962).

J.-L. Colliot-Thélène
Université de Paris-Sud
Mathématique - Bât. 425
91405 ORSAY CEDEX
FRANCE