Points rationnels sur les fibrations

Notes pour un cours donné à Budapest en septembre 2001

J.-L. Colliot-Thélène

Introduction

On trouvera ici une description de résultats récents sur les points rationnels des variétés algébriques sur un corps de nombres, obtenus par la méthode de la descente et la méthode des fibrations. Je rappelle quelques notions de base, mais renvoie le lecteur à mon précédent rapport [4] pour une description détaillée de la plupart des résultats obtenus avant 1996.

Le texte comprend trois parties de nature assez différente.

Au chapitre 1, après avoir donné des démonstrations simplifiées d'un certain nombre de résultats de base sur l'obstruction de Brauer-Manin ("lemme formel" de D. Harari), on décrit la descente sur une variété ouverte (utilisée pour la première fois dans [12]) et, simplifiant légèrement l'argument de Heath-Brown et Skorobogatov [24], on l'applique à l'étude des solutions de l'équation

$$t^a(1-t)^b = \varepsilon . N_{K/k}(\mathbf{x})$$

où a et b sont des entiers naturels, $\varepsilon \in k$ est une constante non nulle, t varie dans k et $\mathbf{x}$ dans un corps K extension finie de k, et $N_{K/k}$ est la norme de K à k. Dans ce chapitre on s'est efforcé de donner des démonstrations complètes.

Tel n'est pas le cas au chapitre 2, où l'on évoque les résultats obtenus par une méthode inventée par Swinnerton-Dyer [35] et perfectionnée dans [14], qui vise à assurer l'existence de (beaucoup de) points rationnels sur une variété que l'on peut fibrer sur la droite projective, les fibres étant des espaces homogènes principaux de variétés abéliennes. Le principe de la méthode est décrit, mais le détail de l'exécution finale est très élaboré et ne saurait être complètement détaillé. On énonce ensuite les principaux résultats obtenus par cette méthode. Un résultat particulièrement frappant a été ainsi obtenu par Swinnerton-Dyer ([39]) : supposant les groupes de Tate-Shafarevich de courbes elliptiques finis (une conjecture bien connue), il montre que le principe de Hasse vaut pour les hypersurfaces cubiques diagonales de dimension au moins 3 sur le corps des rationnels.

La finitude des groupes de Tate-Shafarevich des variétés abéliennes sur un corps de nombres a un analogue, dû à Tate, sur les corps de fonctions $\mathbf{F}_q(C)$ d'une variable sur un corps fini $\mathbf{F}_q$. Des cas particuliers de cet analogue sont connus. Au chapitre 3, qui est original, je montre que ces cas particuliers suffisent pour établir de façon *inconditionnelle* l'analogue fonctionnel du résultat de Swinnerton-Dyer : *Sur un corps de fonctions* $\mathbf{F}_q(C)$ *avec* q *impair et* $q \equiv 2$ mod. 3*, le principe de Hasse vaut pour les hypersurfaces cubiques diagonales de dimension au moins* 3. La lecture de ce chapitre présuppose celle de [39].

Je remercie David Harari, Alexei Skorobogatov et Peter Swinnerton-Dyer pour leurs commentaires sur des versions préliminaires de ce texte.

Commençons par quelques rappels (pour plus de détails, voir [4]).

Accouplement de Brauer-Manin

Le groupe de Brauer (cohomologique) d'un schéma X est le groupe $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbf{G}_m)$. On supposera le lecteur familier avec la série de trois textes de Grothendieck [16], ou du moins avec les propriétés de base du groupe de Brauer (voir [15], §1). Etant donnés k un corps, $\overline{k}$ une clôture séparable de k, Γ le groupe de Galois de $\overline{k}$ sur k, puis X une k-variété (c'est-à-dire un k-schéma séparé de type fini), et $\overline{X} = X \times_k \overline{k}$, on note $\mathrm{Br}_1(X) = \mathrm{Ker}[\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})]$. On a la suite exacte naturelle

$$H^2(\Gamma, \overline{k}[X]^*) \to \mathrm{Br}_1(X) \to H^1(\Gamma, \mathrm{Pic}(\overline{X})),$$

où $\overline{k}[X]^*$ désigne le groupe des unités de $\overline{X}$ et $\mathrm{Pic}(\overline{X})$ est le groupe de Picard de $\overline{X}$.

Rappelons la définition de l'obstruction de Brauer-Manin (pour plus de détails, voir par exemple [4], §1). Soit k un corps de nombres. Notons Ω l'ensemble des places de k. Rappelons ce qu'est l'ensemble $X(\mathbf{A}_k)$ des adèles d'une k-variété X. On choisit un modèle $\mathcal{X}/O$ de X au-dessus d'un ouvert $\mathrm{Spec}(O)$ du spectre de l'anneau des entiers du corps de nombres k, c'est-à-dire un schéma $\mathcal{X}$ plat et de type fini sur O, de fibre générique X/k. On note S l'ensemble fini des places de k non dans cet ouvert. L'ensemble $X(\mathbf{A}_k) \subset \prod_{v \in \Omega} X(k_v)$ est la réunion, pour T variant parmi les sous-ensembles finis de Ω avec $S \subset T$, des sous-ensembles $\prod_{v \in T} X(k_v) \times \prod_{v \notin T} \mathcal{X}(O_v)$ de $\prod_{v \in \Omega} X(k_v)$. Cette définition ne dépend pas du choix du modèle $\mathcal{X}$. On munit $X(\mathbf{A}_k)$ de la topologie de produit restreint, dont une base d'ouverts est formée des ensembles de la forme $\prod_{v \in T} U_v \times \prod_{v \notin T} \mathcal{X}(O_v)$, avec T comme ci-dessus et U_v ouvert de $X(k_v)$. Si X est propre sur k, l'espace $X(\mathbf{A}_k)$ est simplement le produit topologique des $X(k_v)$ pour v dans Ω.

La théorie du corps de classes permet de définir un accouplement (dit de Brauer-Manin)

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

entre l'ensemble des adèles de X, supposé non vide, et le groupe de Brauer $\mathrm{Br}(X)$ de X. A une adèle $\{P_v\} \in X(\mathbf{A}_k)$ et à $A \in \mathrm{Br}(X)$ on associe la somme (finie) $\sum_{v \in \Omega} A(P_v)$. Ici $A(P_v) \in \mathrm{Br}(k_v)$ est identifié à un élément de $\mathbf{Q}/\mathbf{Z}$ par la théorie du corps de classes local. Pour $B \subset \mathrm{Br}(X)$, on note $X(\mathbf{A}_k)^B$ le fermé de $X(\mathbf{A}_k)$ sur lequel les éléments de B s'annulent. On note $X(\mathbf{A}_k)^{\mathrm{Br}} = X(\mathbf{A}_k)^{\mathrm{Br}(X)}$.

Comme remarqué par Manin, la théorie du corps de classes global (loi de réciprocité) montre que l'image diagonale de $X(k)$ dans $X(\mathbf{A}_k)$ est incluse dans $X(\mathbf{A}_k)^{\mathrm{Br}}$. En particulier, si $X(\mathbf{A}_k)^{\mathrm{Br}} = \emptyset$, alors $X(k) = \emptyset$: c'est l'obstruction de Brauer-Manin au principe de Hasse. L'adhérence de $X(k)$ dans $X(\mathbf{A}_k)$ pour la topologie adélique est aussi contenue dans $X(\mathbf{A}_k)^{\mathrm{Br}}$. Il est intéressant de trouver des classes de variétés pour lesquelles cette dernière inclusion est une bijection : on dit alors que l'obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible est la seule pour ces variétés. Lorsque X est projective et que le quotient $\mathrm{Br}(X)/\mathrm{Br}(k)$ est fini, cette propriété implique l'approximation faible-faible : il existe un ensemble fini de places S_0 de k tel que pour tout ensemble fini T de places disjoint de S_0, l'image diagonale de $X(k)$ dans $\prod_{v \in T} X(k_v)$ est dense.

Il était déraisonnable d'espérer que cette obstruction au principe de Hasse fût la seule pour toutes les variétés (géométriquement connexes) projectives et lisses. C'est cependant récemment que Skorobogatov [33] a exhibé le premier exemple de telle variété X satisfaisant $X(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$ mais néanmoins $X(k) = \emptyset$. La variété considérée est une surface bielliptique. De même, il était déraisonnable d'espérer que cette obstruction fût, pour de telles variétés, la seule obstruction à l'approximation faible. Inspiré par [33], Harari [19] montra comment fabriquer de nombreux exemples de k-variétés projectives et lisses X pour lesquelles le groupe de Brauer $\mathrm{Br}(X)$ ne suffit pas à rendre compte du défaut d'approximation faible. L'obstruction qu'il utilise repose sur l'existence de revêtements finis étales galoisiens $Y \to X$, et plus généralement de G-torseurs sur X, pour G un k-groupe algébrique fini. Lorsque le groupe G est abélien, on peut réinterpréter l'obstruction en termes du groupe de Brauer de X, mais il n'en est pas ainsi en général. D'où de nombreux exemples lorsque le groupe fondamental géométrique de X n'est pas abélien. Puis Harari et Skorobogatov [21] montrèrent que l'exemple de [33] peut s'interpréter de ce point de vue. (Harari [20] montre par contre qu'on ne peut espérer fabriquer de tels exemples au moyen de torseurs sous un k-groupe G linéaire connexe.)

Il reste néanmoins des classes très intéressantes de variétés pour lesquelles on espère que l'obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible est la seule. Je renvoie en particulier le lecteur à la conjecture 1 de [4] (p. 25) (noter que le commentaire suivant cette conjecture n'a plus lieu d'être, le travail cité dans ce commentaire étant erroné). Sansuc et moi-même avons conjecturé que l'obstruction de Brauer-Manin est la seule pour les surfaces (géométriquement) rationnelles; on peut se demander si plus généralement il en est ainsi pour les variétés (géométriquement) rationnellement connexes (pour la définition de ces dernières, voir le texte de C. Araujo et J. Kollár dans ce volume).

Fibrations

Soient k un corps de caractéristique zéro, X une k-variété projective et lisse, géométriquement intègre, et $p : X \to \mathbf{P}^1_k$ un k-morphisme dominant. Etant donné un point $M \in \mathbf{P}^1_k$, de corps résiduel $k(M)$, on note $X_M/k(M)$ la fibre de p en M. On note η le point générique de $\mathbf{P}^1_k$; son corps résiduel est le corps des fonctions $K = k(\mathbf{P}^1)$ de $\mathbf{P}^1_k$. La fibre générique X_η/K de p est lisse. La fibre générique géométrique est $X_\eta \times_K K_s$, où K_s est une clôture algébrique de K. On supposera cette fibre géométrique intègre. On dira alors que p est une *fibration*.

On va s'intéresser aux fibrations p satisfaisant la propriété : pour tout point fermé $M \in \mathbf{P}^1_k$, la fibre $X_M/k(M)$ possède une composante de multiplicité un (en d'autres termes toute fibre géométrique possède une composante de multiplicité un, en d'autres termes encore la fibration p est localement scindée pour la topologie étale sur $\mathbf{P}^1_k$).

On sera amené à considérer le sous-groupe $\mathrm{Br}_{\mathrm{vert}}(X/\mathbf{P}^1_k)$ du groupe de Brauer de X, groupe qu'on appellera "groupe de Brauer vertical" (par rapport à la fibration p). C'est par définition le groupe des éléments de $\mathrm{Br}(X)$ dont la restriction à la fibre générique $X_\eta/k(\mathbf{P}^1)$ provient de $\mathrm{Br}(k(\mathbf{P}^1))$. Sous l'hypothèse de multiplicité un faite sur les fibres, le quotient $\mathrm{Br}_{\mathrm{vert}}(X/\mathbf{P}^1_k)/\mathrm{Br}(k)$ est fini.

Pour de telles fibrations, lorsque k est un corps de nombres, on essaye de trouver des points rationnels sur la k-variété X en se servant des propriétés arithmétiques des fibres de p au-dessus des points k-rationnels.

L'expérience montre que la difficulté de cette entreprise croît avec l'invariant $\delta = \delta(p)$ d'une telle fibration ([32], [4]). Rappelons-en la définition. C'est la somme des degrés $[k(M) : k]$ des points fermés $M \in \mathbf{P}^1_k$ tels que la fibre $X_M/k(M)$ ne soit pas "scindée", c'est-à-dire ne possède pas de composante de multiplicité un géométriquement intègre sur $k(M)$.

Théorème 0.1 *Soit $p : X \to \mathbf{P}^1_k$ une fibration comme ci-dessus. Dans chacun des cas suivants, l'obstruction de Brauer-Manin au principe de Hasse est la seule pour X :*

(i) [17] [18] *On a $\delta(p) \leq 1$, la fibre générique X_η de p satisfait $H^i(X_\eta, O_{X_\eta}) = 0$ pour $i = 1, 2$, le groupe de Néron-Severi de la fibre générique géométrique est sans torsion, et l'on suppose que l'obstruction de Brauer-Manin est la seule pour les fibres lisses de p au-dessus des points rationnels.*

(ii) [13] [12] *On a $\delta(p) \leq 2$, et l'on suppose la validité du principe de Hasse pour les fibres de p au-dessus des points rationnels.*

(iii) [15] [13] *(énoncé conditionnel) Le principe de Hasse vaut pour les fibres de p au-dessus des points rationnels; pour tout point fermé $M \in \mathbf{P}^1_k$, il existe une composante intègre Y de multiplicité un de $X_M/k(M)$ telle que la clôture intégrale de $k(M)$ dans le corps des fonctions de Y soit une extension abélienne de k; l'entier $\delta(p)$ est quelconque, mais l'on suppose la validité de l'hypothèse de Schinzel.*

L'hypothèse de Schinzel est une extension audacieuse du théorème de Dirichlet sur les premiers dans une progression arithmétique, dont c'est le seul cas connu. Un cas particulier de cette hypothèse est la conjecture des nombres premiers jumeaux.

L'énoncé (iii) ci-dessus est un cas particulier du résultat suivant.

Théorème 0.2 [13] *Soit $p : X \to \mathbf{P}^1_k$ une fibration comme ci-dessus. Supposons que pour tout point fermé $M \in \mathbf{P}^1_k$ la fibre $X_M/k(M)$ possède une composante Y de multiplicité un telle que la clôture intégrale de $k(M)$ dans le corps des fonctions de Y est une extension abélienne de $k(M)$. Supposons qu'il existe une adèle $\{P_v\} \in X(\mathbf{A}_k)$ orthogonal à $\mathrm{Br}_{\mathrm{vert}}(X/\mathbf{P}^1_k)$ pour l'accouplement de Brauer-Manin. Supposons satisfaite l'une des deux hypothèses :*

(a) pour tout point fermé $M \in \mathbf{P}^1_k$ sauf au plus deux points rationnels, la fibre X_M possède une composante de multiplicité un géométriquement intègre sur $k(M)$ (en particulier $\delta(p) \leq 2$);

(b) $\delta(p)$ est quelconque, mais l'on admet l'hypothèse de Schinzel.

Alors il existe une infinité de points $M \in \mathbf{P}^1(k)$ tels que $X_M(\mathbf{A}_k) \neq \emptyset$. Plus précisément, l'ensemble des points $M \in \mathbf{P}^1(k)$ dont la fibre X_M est lisse et satisfait $X_M(\mathbf{A}_k) \neq \emptyset$ est dense dans $p(X(\mathbf{A}_k)^{\mathrm{Br}_{\mathrm{vert}}}) \subset \mathbf{P}^1(\mathbf{A}_k)$.

La démonstration de (a) est un cas particulier de celle de (b): elle utilise le théorème de la progression arithmétique.

Le théorème 0.2 ramène dans une certaine mesure l'étude du principe de Hasse pour X à celui du principe de Hasse pour les fibres de p. Dans ce rapport, on s'intéresse au cas où la fibre générique de p est une compactification lisse d'un espace homogène sous un groupe algébrique connexe.

Un cas est particulièrement agréable : c'est celui où cette fibre générique est une variété projective espace homogène d'un groupe linéaire connexe. Dans ce cas les fibres au-dessus de points rationnels satisfont le principe de Hasse (Harder). Sous les hypothèses du théorème on conclut que l'obstruction de Brauer-Manin verticale est la seule obstruction pour la k-variété X.

Un autre cas intéressant (et difficile) est le suivant. Considérons une extension finie de corps de nombres K/k, une base $\omega_i, i = 1, \cdots, n$ de K sur k, et un polynôme non nul $P(t) \in k[t]$. Notons $N_{K/k}$ la norme de K à k. L'hypersurface affine définie par l'équation

$$P(t) = N_{K/k}(\sum_{i=1}^{n} x_i \omega_i)$$

dans l'espace affine $\mathbf{A}^{n+1}_k$ admet un modèle projectif et lisse X équipé d'une fibration $p : X \to \mathbf{P}^1_k$ étendant la projection sur la coordonnée t. Une fibre générale de p est une compactification lisse d'un espace principal homogène sous le k-tore $R^1_{K/k}\mathbf{G}_m$ des éléments de K^* de norme 1. L'invariant $\delta = \delta(p)$ est inférieur ou égal (et souvent égal) au nombre de racines distinctes de P, augmenté de 1. Sauf si $P(t)$ n'a qu'une seule racine, on aura donc en général $\delta(p) \geq 3$, et on ne pourra pas appliquer le théorème 0.1 (ii). On peut néanmoins conjecturer que dans ce cas l'adhérence de $X(k)$ dans $X(\mathbf{A}_k)$ coïncide avec $X(\mathbf{A}_k)^{\mathrm{Br}}$. C'est connu dans les cas suivants :

(i) $[K : k] = 2$ et $P(t)$ est de degré 3 ou 4 ([11]) ($\delta = 4$).

(ii) $[K : k] = 3$ et $P(t)$ est de degré au plus 3 ([9]) ($\delta = 3$).

(iii) L'extension K/k est cyclique et l'on accepte l'hypothèse de Schinzel (application du théorème 0.2). Ici δ est quelconque.

(iv) Le corps k est le corps des rationnels, l'extension K/k est quelconque, $P(t) = \varepsilon t^a(1-t)^b$ avec $\varepsilon \in k^*$, et $(a, b) = 1$ ([24], théorème 1.7 ci-après). Ici $\delta = 3$.

Dans chacun des trois premiers cas, d'une part $\mathrm{Br}_{\mathrm{vert}}(X/\mathbf{P}^1_k) = \mathrm{Br}(X)$, d'autre part le principe de Hasse vaut pour les fibres. Il n'en est pas de même dans le cas (iv).

Chapitre 1 : La descente ouverte

Accouplement de Brauer-Manin et variétés ouvertes

Proposition 1.1 *Soient k un corps de nombres et X une k-variété algébrique. Soit* $\mathrm{Spec}(O)$ *un ouvert du spectre de l'anneau des entiers de k et $\mathcal{X}/O$ un O-schéma de type fini, de fibre générique $X/\mathrm{Spec}(k)$. Etant donné un sous-ensemble fini $B \subset \mathrm{Br}(X)$, pour presque toute place $v \in \mathrm{Spec}(O)$, on a $\alpha(M_v) = 0$ pour tout $\alpha \in B$ et tout $M_v \in \mathcal{X}(O_v)$.*

Démonstration Quitte à restreindre $\mathrm{Spec}(O)$, on peut supposer que chaque $\alpha \in B$ provient d'un élément $\mathcal{A} \in \mathrm{Br}(\mathcal{X})$ (passage à la limite en cohomologie étale). La nullité du groupe de Brauer $\mathrm{Br}(O_v)$ de l'anneau des entiers de O_v (anneau des entiers du complété k_v pour v place finie) permet de conclure.

Proposition 1.2 *Soient k un corps de nombres et X une k-variété algébrique propre. Soit $\alpha \in \mathrm{Br}(X)$. Pour presque toute place v de k, pour tout $M_v \in X(k_v)$, on a $\alpha(M_v) = 0$.*

Démonstration Il existe un ouvert $\mathrm{Spec}(O)$ du spectre de l'anneau des entiers de k et $\mathcal{X}/O$ un O-schéma propre de fibre générique X/k, tel que de plus α provienne d'un élément $\mathcal{A} \in \mathrm{Br}(\mathcal{X})$. Pour toute place $v \in \mathrm{Spec}(O)$, on a $X(k_v) = \mathcal{X}(O_v)$ (propreté). Pour $M_v \in X(k_v)$, notons $\tilde{M}_v$ le point correspondant de $\mathcal{X}(O_v)$. L'élément $\alpha(M_v) \in \mathrm{Br}(k_v)$ est l'image de $\mathcal{A}(\tilde{M}_v) \in \mathrm{Br}(O_v)$, et $\mathrm{Br}(O_v) = 0$.

L'énoncé suivant, connu et utilisé auparavant dans des cas particuliers, est dû à D. Harari [17]. J'en donne ici une démonstration simplifiée.

Théorème 1.3 (Harari, [17], Théorème 2.1.1 p. 226) *Soient k un corps de nombres et X une k-variété lisse connexe. Soit $\mathcal{X}/O$ un modèle entier de X au-dessus d'un ouvert* $\mathrm{Spec}(O)$ *du spectre de l'anneau des entiers de k. Soit $U \subset X$ un ouvert de X. Pour tout élément $\alpha \in \mathrm{Br}(U)$ qui n'est pas dans $\mathrm{Br}(X) \subset \mathrm{Br}(U)$, il existe une infinité de places v de k pour lesquelles il existe $M_v \in U(k_v) \cap \mathcal{X}(O_v)$ avec $\alpha(M_v) \neq 0$.*

Démonstration Il existe une sous-variété fermée intègre $Z \subset X$, de codimension un, de point générique ζ, telle que le résidu $\partial_\zeta(\alpha) \in H^1(k(Z), \mathbf{Q}/\mathbf{Z})$ au point générique de Z soit non nul. Quitte à remplacer X par un ouvert, on peut supposer que Z est lisse sur k, que α n'a qu'un seul résidu non trivial sur X, à savoir celui en ζ, et que le résidu $\partial_\zeta(\alpha)$ appartient à $H^1(Z, \mathbf{Q}/\mathbf{Z}) \subset H^1(k(Z), \mathbf{Q}/\mathbf{Z})$ (la cohomologie utilisée est la cohomologie étale). Quitte à restreindre Z, on peut supposer que Z est un revêtement fini d'un espace affine $\mathbf{A}^d_k$. Soit Z_1/Z le revêtement fini (cyclique) défini par $\partial_\zeta(\alpha)$. Le théorème d'irréductibilité de Hilbert, appliqué au revêtement composé $Z_1/\mathbf{A}^d_k$, assure l'existence de points k-rationnels de $\mathbf{A}^d_k$ dont la fibre est intègre. Choisissons un tel k-point. Son image réciproque par l'appplication $Z \to \mathbf{A}^d_k$ est un point fermé $P \in Z$ tel que $\partial_\zeta(\alpha)(P) \in H^1(k(P), \mathbf{Q}/\mathbf{Z})$ est non nul.

On peut compléter l'équation locale de $Z \subset X$ en P par un système régulier de paramètres de l'anneau local régulier $O_{X,P}$. On trouve ainsi une courbe fermée intègre $C \subset X$, passant par P, lisse en P, et transverse à Z en P. Quitte à restreindre encore X, on peut supposer C/k lisse et $Z \cap C = P$. Les réductions opérées assurent que α appartient à $\mathrm{Br}(X \setminus Z)$. Ainsi α induit un élément $\alpha_C \in \mathrm{Br}(C \setminus P)$. De la transversalité de C et Z on tire l'égalité

$$\partial_P(\alpha_C) = \partial_\zeta(\alpha)(P) \in H^1(k(P), \mathbf{Q}/\mathbf{Z}).$$

Ainsi $\partial_P(\alpha_C) \neq 0$. Comme l'inclusion $C \subset X$ s'étend à une inclusion de modèles entiers sur un ouvert convenable du spectre de l'anneau des entiers de k, on est réduit à établir l'énoncé pour une k-courbe lisse connexe.

On considère dorénavant une k-courbe lisse connexe (donc intègre) C, un point fermé $P \in C$, on note $U = C \setminus P$, et on se donne $\alpha \in \mathrm{Br}(U)$ de résidu $\chi = \partial_P(\alpha) \in H^1(k(P), \mathbf{Q}/\mathbf{Z})$ non nul. Soit $r > 1$ l'ordre de $\partial_P(\alpha)$. On a donc $\partial_P(\alpha) \in H^1(k(P), \mathbf{Z}/r) \subset H^1(k(P), \mathbf{Q}/\mathbf{Z})$. Quitte à restreindre C, on peut supposer C affine, soit $C = \mathrm{Spec}(A)$, et P donné par l'annulation de $f \in A$. Soit A_{hs} l'hensélisé de A en P. La restriction $H^1(A_{hs}, \mathbf{Z}/r) \to H^1(k(P), \mathbf{Z}/r)$ est un isomorphisme. Il existe donc un ouvert étale connexe $q : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$, soit $q : D \to C$, tel que $q : Q = q^{-1}(P) \to P$ soit un isomorphisme, et tel que χ soit la restriction de $\xi \in H^1(D, \mathbf{Z}/r)$. Soit $V = D \setminus Q$. Soit $(f, \xi) \in \mathrm{Br}(V)$ la classe obtenue par cup-produit de la classe de $f \in k[V]^*/k[V]^{*r} \subset H^1(V, \mu_r)$ avec la classe $\xi \in H^1(D, \mathbf{Z}/r)$. La différence $\beta = \alpha_D - (f, \xi) \in \mathrm{Br}(V)$ a un résidu trivial en Q, elle appartient donc à $\mathrm{Br}(D)$.

Il existe un ouvert $\mathrm{Spec}(O)$ du spectre de l'anneau des entiers de k, une courbe affine relative $\mathcal{C}/\mathrm{Spec}(O)$ (plate et de type fini), une courbe affine relative $\mathcal{D}/\mathrm{Spec}(O)$ (plate et de type fini), un morphisme $\mathcal{D} \to \mathcal{C}$, étendant la situation $D/C/\mathrm{Spec}(k)$, tels que f provienne d'un élément, encore noté f, de l'anneau de $\mathcal{C}$, que $\xi \in H^1(D, \mathbf{Z}/r)$ soit la restriction d'un élément $\xi \in H^1(\mathcal{D}, \mathbf{Z}/r)$, que $\beta \in \mathrm{Br}(D)$ soit la restriction d'un élément $\beta \in \mathrm{Br}(\mathcal{D})$. On peut en outre supposer que les fermés de $\mathcal{D}$ et de $\mathcal{C}$ définis par $f = 0$ sont intègres et isomorphes via la projection $\mathcal{D} \to \mathcal{C}$, et que la projection naturelle de ces fermés vers $\mathrm{Spec}(O)$ est finie et étale. Soit R l'anneau dont le spectre est le fermé défini par $f = 0$ dans $\mathcal{C}$ (et dans $\mathcal{D}$). Le corps des fractions de R est le corps $k(P)$.

Le théorème de Tchebotarev assure l'existence d'une infinité de places v de k telles qu'il existe une place w de $k(P)$ avec $k_v \simeq k(P)_w$ (i.e. w est de degré un sur v) et w inerte dans l'extension cyclique $k(P)(\chi)/k(P)$ définie par $\chi \in H^1(k(P), \mathbf{Z}/r)$ ([17], Prop. 2.2.1, p. 226).

Pour un tel couple v, il existe un O_v-point N_v^0 du fermé $f = 0$ de $\mathcal{D}$ qui s'envoie isomorphiquement sur un O_v-point M_v^0 de $\mathcal{C}$.

Soit $N_v \in \mathcal{D}(O_v)$ tel que $f(N_v) \neq 0$ et soit $M_v \in \mathcal{C}(O_v) \subset C(k_v)$ son image. On a

$$\alpha(M_v) = \alpha(N_v) = \beta(N_v) + (f(N_v), \chi(N_v)) \in \mathrm{Br}(k_v) \simeq \mathbf{Q}/\mathbf{Z}.$$

On a $\beta(N_v) \in \mathrm{Br}(O_v) = 0$. Par ailleurs, comme w est inerte dans l'extension cyclique $k(P)(\chi)/k(P)$, si N_v est suffisamment proche de N_v^0 pour la topologie v-adique sur $\mathcal{D}(O_v)$, la classe $\chi(N_v) \in H^1(k(P)_w, \mathbf{Z}/r) = H^1(k_v, \mathbf{Z}/r)$ est d'ordre r. La formule standard pour le symbole modéré montre alors que $\alpha(M_v) \in \mathbf{Z}/r \subset \mathbf{Q}/\mathbf{Z}$ est égal à la classe de la valuation $v(f(N_v))$ modulo r. Comme le fermé $f = 0$ de $\mathcal{D} \times_O O_v$ contient la O_v-section de $\mathcal{D} \times_O O_v \to \mathrm{Spec}(O_v)$ définie par N_v^0, on peut trouver $N_v \in \mathcal{D}(O_v)$, proche de N_v^0, tel que $v(f(N_v)) \equiv 1 \bmod r$, et donc d'image $M_v \in \mathcal{C}(O_v) \subset C(k_v)$ satisfaisant $\alpha(M_v) \neq 0$.

Remarques

(i) Le cas le plus simple est le suivant, que le lecteur devrait établir lui-même avant de lire la démonstration ci-dessus. On considère $a \in k^*$, a non carré dans k, on prend $X = \mathbf{A}^1_k = \mathrm{Spec}(k[t])$, puis U l'ouvert défini par $t \neq 0$, enfin $\alpha \in \mathrm{Br}(k(t))$ la classe de l'algèbre de quaternions (a, t). Il existe une infinité de places v pour lequelles il existe $t_v \in k_v^*$ avec $(a, t_v) \neq 0 \in \mathrm{Br}(k_v)$.

(ii) Sur cet exemple, il existe aussi une infinité de places v telle que α s'annule identiquement sur $U(k_v)$. Ce sera plus généralement le cas pour tout X de dimension un. Par contre, si X est géométriquement intègre de dimension au moins 2 et qu'il existe un point de codimension un de X où A a un résidu $\partial(A) \in H^1(k(Z), \mathbf{Q}/\mathbf{Z})$ définissant une extension cyclique $L/k(Z)$ telle que k soit algébriquement clos dans L (possible seulement si la dimension de X est au moins 2), alors pour presque toute place v de k la classe α prend sur $U(k_v)$ au moins une valeur autre que 0.

Des propositions précédentes, par un argument essentiellement combinatoire, on établit l'énoncé fort utile suivant, qui est une variante, énoncée dans [12], du "lemme formel" de D. Harari (Corollaire 2.6.1, p. 233 de [17]).

Théorème 1.4 *Soient k un corps de nombres et X une k-variété lisse et géométriquement connexe. Soit $U \subset X$ un ouvert non vide, et soit $B \subset \mathrm{Br}(U)$ un sous-groupe fini. Soit $\{P_v\} \in U(\mathbf{A}_k)$. Supposons que pour tout α dans le groupe fini $B \cap \mathrm{Br}(X)$, on ait*

$$\sum_{v \in \Omega} \alpha(P_v) = 0.$$

Alors pour tout ensemble fini S de places de k il existe une adèle $\{M_v\} \in U(\mathbf{A}_k)$ telle que $M_v = P_v$ pour $v \in S$ et tel que pour tout $\beta \in B$ on ait

$$\sum_{v \in \Omega} \beta(M_v) = 0.$$

Démonstration Comme le groupe B est fini, quitte à remplacer S par un ensemble fini de places plus gros, ce qui est licite, on peut supposer que l'inclusion $U \subset X$ admet un modèle entier $\mathcal{U} \subset \mathcal{X}$ au-dessus de l'anneau O des S-entiers de k tel que $P_v \in \mathcal{U}(O_v) \subset \mathcal{X}(O_v)$ pour $v \notin S$, que $B \subset \mathrm{Br}(\mathcal{U})$ et $B \cap \mathrm{Br}(X) \subset \mathrm{Br}(\mathcal{X})$. Pour tout $\beta \in B$, et pour $v \notin S$, on a $\beta(P_v) = 0$. Pour tout $\beta \in B \cap \mathrm{Br}(X)$, tout $v \notin S$ et tout $M_v \in \mathcal{X}(O_v) \subset X(k_v)$, on a $\beta(M_v) = 0$.

Soit $\alpha \in B, \alpha \notin \mathrm{Br}(X)$. D'après le théorème 1.3, il existe un ensemble infini T_α de places $v \notin S$ et une famille $\{N_v\} \in \prod_{v \in T_\alpha} U(k_v) \cap \mathcal{X}(O_v)$ telle que $\alpha(N_v) \neq 0$ pour tout $v \in T_\alpha$. Le groupe $B/(B \cap \mathrm{Br}(X))$ est fini, donc aussi son dual $\mathrm{Hom}(B/(B \cap \mathrm{Br}(X)), \mathbf{Q}/\mathbf{Z})$. Il existe donc un sous-ensemble infini de T_α tel que les applications linéaires $B/(B \cap \mathrm{Br}(X)) \to \mathbf{Q}/\mathbf{Z}$ données par $\gamma \to \gamma(N_v)$ pour v dans ce sous-ensemble coïncident. Quitte a remplacer T_α par ce sous-ensemble, on peut donc supposer qu'il existe une application linéaire $\varphi_\alpha : B/(B \cap \mathrm{Br}(X)) \to \mathbf{Q}/\mathbf{Z}$ satisfaisant $\varphi_\alpha(\alpha) \neq 0$, telle que pour tout $\beta \in B/(B \cap \mathrm{Br}(X))$, et tout $v \in T_\alpha$, on ait

$$\varphi_\alpha(\beta) = \beta(N_v) \in \mathbf{Q}/\mathbf{Z},$$

avec $N_v \in U(k_v) \cap \mathcal{X}(O_v)$ comme ci-dessus.

Dans le groupe dual du groupe fini $B/(B \cap \mathrm{Br}(X))$, les sommes de telles applications φ_α pour α variant dans $B/(B \cap \mathrm{Br}(X))$ (les répétitions étant autorisées) forment un sous-groupe, que nous notons C; cela résulte simplement du fait que le groupe $B/(B \cap \mathrm{Br}(X))$ est, comme B, un groupe de torsion. Considérons alors l'accouplement naturel bilinéaire $B/(B \cap \mathrm{Br}(X)) \times C \to \mathbf{Q}/\mathbf{Z}$. D'après ce qu'on a vu ci-dessus, cet accouplement de groupes abéliens finis est non dégénéré à gauche. Ainsi le groupe $B/(B \cap \mathrm{Br}(X))$ s'injecte dans le dual de C. Par comptage, ceci n'est possible que si C est égal au dual de $B/(B \cap \mathrm{Br}(X))$ tout entier.

L'hypothèse du théorème assure que la famille $\{P_v\}_{v \in S}$ définit une application linéaire $B/(B \cap \mathrm{Br}(X)) \to \mathbf{Q}/\mathbf{Z}$, donnée par $\beta \mapsto -\sum_{v \in S} \beta(P_v)$. D'après ce qu'on vient de voir, cette application linéaire peut s'écrire comme une somme d'applications φ_α (avec répétitions). On peut écrire chacun des termes de cette dernière somme sous la forme $\beta \mapsto \beta(N_v)$, cette fois-ci sans répétition sur les places v (puisqu'à chaque fois on a une infinité de places à disposition). On a alors trouvé un ensemble T fini de places $v \notin S$ et des points $N_v \in U(k_v) \cap \mathcal{X}(O_v)$ pour $v \in T$ tels que

$$\sum_{v \in S} \beta(P_v) + \sum_{v \in T} \beta(N_v) = 0$$

pour tout $\beta \in B/(B \cap \mathrm{Br}(X))$, soit encore

$$\sum_{v \in S} \beta(P_v) + \sum_{v \in T} \beta(N_v) = 0$$

pour tout $\beta \in B$. On a alors

$$\sum_{v \in S} \beta(P_v) + \sum_{v \in T} \beta(N_v) + \sum_{v \notin S \cup T} \beta(P_v) = 0$$

pour tout $\beta \in B$. Ce qui établit l'énoncé, en choisissant $M_v = N_v$ pour $v \in T$ et $M_v = P_v$ pour $v \notin S \cup T$.

Liens entre torseurs et groupe de Brauer ([10], [12], [33], [34])

On donne ici une version résumée de la théorie de la descente. Jusqu'à une date récente, on se limitait à appliquer ladite méthode aux variétés projectives. C'était le cadre adopté dans [10] (chapitre III) et [33]. L'observation que l'on peut aussi faire des descentes utiles sur des variétés "ouvertes" est récente ([12]).

Soient k un corps et G un k-groupe algébrique lisse. Soit X une k-variété. Par définition, un torseur sur X sous G est une k-variété Y équipée d'un k-morphisme $p : Y \to X$, d'une action $G \times_k Y \to Y$, notée $(g,y) \mapsto g.y$; on a donc $g_1.(g_2.y) = (g_1.g_2).y$, et $e.y = y$, où e désigne l'élément neutre de G. On demande que l'action $G \times_k Y \to Y$ respecte la projection $p : Y \to X$, et on demande que l'action soit fidèle et transitive dans les fibres de p. En d'autres termes, on veut que le morphisme naturel $G \times_k Y \to Y \times_X Y$ défini par $(g,y) \to (gy,y)$ soit un isomorphisme.

On s'intéressera ici seulement au cas d'un k-groupe G commutatif. Sous des hypothèses raisonnables (par exemple G groupe linéaire), le groupe (abélien) de cohomologie étale $H^1(X,G)$ classifie les G-torseurs sur X (à isomorphisme non unique près).

Dans la suite on s'intéresse au cas où le groupe G est un k-groupe de type multiplicatif, c'est-à-dire un k-groupe algébrique qui sur une clôture séparable $\overline{k}$ de k se plonge dans un produit de groupes multiplicatifs $\mathbf{G}_m$. On note $\hat{G} = \mathrm{Hom}_{k-\mathrm{groupes}}(G, \mathbf{G}_m)$ le groupe des caractères d'un tel groupe. Le groupe (des $\overline{k}$-points) de $\hat{G}$ est un groupe abélien de type fini muni d'une action continue de $\Gamma = \mathrm{Gal}(\overline{k}/k)$, pour la topologie discrète sur ce groupe abélien de type fini : l'action de Γ se factorise par un quotient fini. On sait que le foncteur contravariant défini par $G \mapsto \hat{G}$ est une antidualité, qui tranforme suites exactes en suites exactes.

Soient X une k-variété et G un k-groupe de type multiplicatif. Soit Y un G-torseur sur X. A tout caractère $\chi : \overline{G} \to \mathbf{G}_{m,\overline{k}}$, on associe le produit contracté $\overline{Y} \overset{\overline{G}}{\times} \mathbf{G}_{m,\overline{k}}$, qui est un $\mathbf{G}_{m,\overline{k}}$-torseur sur $\overline{X}$. Comme tout torseur pour la topologie étale sous $\mathbf{G}_m$ est localement trivial pour la topologie de Zariski (théorème 90 à la Grothendieck), on obtient ainsi un élément de $\mathrm{Pic}(\overline{X})$. En termes de groupes de cohomologie, on a un homomorphisme naturel

$$\chi : H^1(X,G) \to \mathrm{Hom}_\Gamma(\hat{G}, \mathrm{Pic}(\overline{X})).$$

L'image $\chi([Y])$ de la classe $[Y]$ du torseur Y par cette application est appelée le *type* du torseur Y, elle est souvent simplement notée $\chi(Y)$.

L'énoncé suivant est le théorème principal de la théorie de la descente.

Théorème 1.5 *Soient k un corps de nombres et X une k-variété géométriquement intègre. Soit $Y \to X$ un torseur sur X sous un k-groupe de type multiplicatif G. Soit $\theta : \hat{G} \to$ $\mathrm{Pic}(\overline{X})$ le type du torseur Y et $\tilde{\theta} : H^1(\Gamma, \hat{G}) \to H^1(\Gamma, \mathrm{Pic}(\overline{X}))$ l'application induite. Soit*

$B_\theta \subset \mathrm{Br}_1(X)$ l'image réciproque de $\tilde{\theta}(H^1(\Gamma,\hat{G})) \subset H^1(\Gamma,\mathrm{Pic}(\overline{X}))$ par l'application naturelle $\mathrm{Br}_1(X) \to H^1(\Gamma,\mathrm{Pic}(\overline{X}))$. Soit $\{P_v\} \in X(\mathbf{A}_k)$ tel que pour tout $\alpha \in B_\theta$ on ait $\sum_{v\in\Omega} \alpha(P_v) = 0$. Alors il existe $\xi \in H^1(k,G)$ tel que le torseur Y^ξ possède une adèle $\{M_v\}$ dont l'image par la projection naturelle $Y^\xi \to X$ soit l'adèle $\{P_v\}$.

Démonstration La famille des fibres $[Y](P_v) \in H^1(k_v,T)$ définit une classe dans le produit restreint $P^1(k,G) \subset \prod_v H^1(k_v,G)$. On dispose de la suite exacte de Poitou-Tate

$$H^1(k,G) \to P^1(k,G) \to H^1(k,\hat{G})^o,$$

où l'application $P^1(k,G) \to H^1(k,\hat{G})^o$ est induite par la somme des applications composées

$$i_v : H^1(k_v,G) \to H^1(k_v,G)^o \to H^1(k,G)^o,$$

la notation A^o désignant le dual $\mathrm{Hom}(A,\mathbf{Q}/\mathbf{Z})$ d'un groupe abélien A. La flèche $H^1(k_v,G) \to H^1(k_v,G)^o$, obtenue par cup-produit et théorie du corps de classes local, est un isomorphisme de groupes finis ([31], II.5.8, Thm. 6 p. 112; [27], I.2.4 p. 35). La flèche $H^1(k_v,G)^o \to H^1(k,G)^o$ est la duale de la restriction $H^1(k,G) \to H^1(k_v,G)$. La suite exacte ci-dessus est une partie d'une suite exacte longue ([27], I.4.20 (b) p. 80, où le produit devrait être remplacé par un produit restreint.)

Une vérification homologique non triviale montre que l'hypothèse d'annulation de la somme $\sum_{v\in\Omega} \alpha(P_v)$ pour tout $\alpha \in B_\theta$ entraîne que la somme $\sum i_v([Y](P_v)) \in H^1(k,\hat{G})^o$ est nulle. De l'exactitude de la suite de Poitou-Tate on tire l'existence d'une classe $-\xi \in H^1(k,G)$ d'image $[Y](P_v) \in P^1(k,G)$. Le torseur tordu Y^ξ (de classe $[Y]+\xi$) a donc une fibre triviale en chacun des P_v. Comme on peut écrire un modèle de G et du torseur $Y \to X$ au-dessus d'un ouvert du spectre de l'anneau des entiers de k, on voit aisément qu'il existe une adèle de Y^ξ d'image $\{P_v\} \in X(\mathbf{A}_k)$.

Note Comme le groupe G est commutatif, on peut se permettre l'abus de langage consistant à noter Y^ξ un torseur défini par torsion du torseur Y par un 1-cocycle (quelconque) de Γ à valeurs dans G et de classe $\xi \in H^1(k,G)$. Le torseur Y^ξ est défini à isomorphisme non unique près.

Le théorème ci-dessus fut d'abord énoncé sous l'hypothèse que T est un tore et que X est projective et lisse ([10]). Il fut établi dans le cas général par Skorobogatov [33]. Il est surtout intéressant (= applicable numériquement) lorsque la k-variété X est projective (ou propre), car alors pour tout élément $A \in \mathrm{Br}(X)$ il existe seulement un nombre fini de places v pour lesquelles l'application d'évaluation $ev_A : X(k_v) \to \mathbf{Q}/\mathbf{Z}$ a une image non réduite à zéro. On peut donc espérer calculer les valeurs prises par $\sum_{v\in\Omega} A(P_v)$ lorsque $\{P_v\}_{v\in\Omega}$ parcourt les adèles de X. Pour les variétés ouvertes, l'énoncé efficace est le suivant ("descente sur une variété ouverte" [12]).

Théorème 1.6 *Soient k un corps de nombres et X une k-variété lisse géométriquement connexe satisfaisant $\overline{k}^* \simeq \overline{k}[X]^*$. Soit $X \subset X_c$ une k-compactification lisse. Soit $Y \to X$ un torseur sur X sous un k-tore T. Soit $\theta : \hat{T} \to \mathrm{Pic}(\overline{X})$ le type du torseur Y et $\tilde{\theta} : H^1(\Gamma,\hat{T}) \to H^1(\Gamma,\mathrm{Pic}(\overline{X}))$ l'application induite. Soit $B_\theta \subset \mathrm{Br}_1(X)$ l'image réciproque de $\tilde{\theta}(H^1(\Gamma,\hat{T})) \subset H^1(\Gamma,\mathrm{Pic}(\overline{X}))$ par l'application naturelle $\mathrm{Br}_1(X) \to H^1(\Gamma,\mathrm{Pic}(\overline{X}))$. Soit $\{P_v\} \in X(\mathbf{A}_k)$ telle que pour tout $\alpha \in B_\theta \cap \mathrm{Br}(X_c)$ on ait $\sum_{v\in\Omega} \alpha(P_v) = 0$. Soit S un ensemble fini de places de k. Alors il existe $\xi \in H^1(k,T)$ tel que le torseur Y^ξ possède une adèle $\{M_v\}$, et que pour chaque $v \in S$ l'image de M_v par la projection structurale $Y^\xi \to X$ soit le point P_v.*

Démonstration Comme T est un k-tore, son groupe des caractères $\hat{T}$ est un groupe abélien libre de type fini, donc le groupe $H^1(\Gamma,\hat{T})$ est fini. Par ailleurs, l'hypothèse $\overline{k}^* \simeq \overline{k}[X]^*$ donne la suite exacte

$$\mathrm{Br}(k) \to \mathrm{Br}_1(X) \to H^1(\Gamma,\mathrm{Pic}(\overline{X})).$$

Le groupe $B_\theta/\mathrm{Br}(k)$ est donc un groupe fini. Soit $B \subset B_\theta$ un groupe fini s'envoyant surjectivement sur $B_\theta/\mathrm{Br}(k)$. L'hypothèse et le théorème 1.4 montrent l'existence d'une adèle $\{R_v\} \in X(\mathbf{A}_k)$ avec $M_v = P_v$ pour $v \in S$, telle que $\sum_{v\in\Omega} \alpha(R_v) = 0$ pour tout $\alpha \in B$, donc aussi pour tout $\alpha \in B_\theta$. Le théorème 1.5 permet de conclure.

Un théorème de Heath-Brown et Skorobogatov

Dans ce paragraphe, je donne une démonstration légèrement simplifiée d'un résultat récent de Heath-Brown et Skorobogatov [24]. Comme chez ces auteurs, la démonstration repose sur la descente sur une variété ouverte.

Théorème 1.7 *Soit K/k une extension finie de corps de nombres, et soit $\omega_1, \cdots, \omega_n$ une base de K/k. Soient a, b des entiers strictement positifs, premiers entre eux, et soit $\varepsilon \in k^*$. Soit U l'ouvert de lissité de la k-variété affine définie par l'équation*

$$t^a(1-t)^b = \varepsilon.N_{K/k}(x_1\omega_1 + \cdots + x_n\omega_n).$$

Soit X une k-compactification lisse de U. Supposons que le corps k est le corps $\mathbf{Q}$ des rationnels. Alors l'ensemble $X(k)$ est dense dans $X(\mathbf{A}_k)^{\mathrm{Br}(X)}$, le fermé de $X(\mathbf{A}_k)$ formé des adèles sur lesquelles s'annule le groupe de Brauer de X. L'adhérence de $X(k)$ dans $X(\mathbf{A}_k)$ est ouverte. L'approximation faible-faible vaut pour X.

Démonstration On vérifie aisément que le lieu singulier de l'hypersurface affine de $\mathbf{A}^{n+1}$ définie par

$$t^a(1-t)^b = \varepsilon.N_{K/k}(x_1\omega_1 + \cdots + x_n\omega_n)$$

est de codimension au moins deux, puis que la flèche naturelle $\overline{k}^* \to \overline{k}[U]^*$ est un isomorphisme : les seules fonctions inversibles sur $\overline{U}$ sont les constantes. Soit $U_1 \subset U$ l'ouvert défini par $t(1-t) \neq 0$. Soit $T = R^1_{K/k}\mathbf{G}_m$ le k-tore des éléments de norme 1 dans K^*. Sur la variété U, le diviseur de la fonction t, et le diviseur de la fonction $1-t$, sont des normes de diviseurs sur U_K : comme U est lisse, il suffit de considérer les diviseurs au sens de Weil, la vérification est immédiate. Ceci implique ([10], Lemme 2.7.6 p. 446 et Exemple 2.7.8 (b)) que pour $r, s \in \mathbf{Z}$, le torseur sous T sur U_1 défini par $t^s(1-t)^r = N_{K/k}(y_1\omega_1 + \cdots + y_n\omega_n) \neq 0$ est la restriction d'un torseur Y sous T sur U. Le type du torseur $Y \to U$ est un Γ-homomorphisme $\theta : \hat{T} \to \mathrm{Pic}(\overline{U})$. Soit $B_\theta \subset \mathrm{Br}_1(U)$ le groupe défini au théorème 1.6.

Soit $\{P_v\} \in X(\mathbf{A}_k)^{\mathrm{Br}(X)}$. On a donc $\{P_v\} \in X(\mathbf{A}_k)^{B_\theta}$. Pour établir le théorème, il suffit de montrer que pour tout ensemble fini S de places et toute famille de voisinages $W_v \subset X(k_v)$ il existe un point $M \in X(k)$ tel que $M_v \in W_v$ pour $v \in S$. Comme $B_\theta/\mathrm{Br}(k)$ est fini, on voit aisément que l'on peut remplacer $\{P_v\}$ par une adèle, encore notée $\{P_v\}$, de l'ouvert $U_1 \subset X$.

L'hypothèse et le théorème 1.6 assurent alors l'existence d'un torseur Y^ξ sur U sous T (de même type que Y), avec $\xi \in k^*/N_{K/k}(K^*) = H^1(k, T)$ convenable, qui possède une adèle $\{M_v\}$ telle que pour tout $v \in S$ l'image par la projection $Y^\xi \to U$ de M_v est P_v.

En appliquant le théorème 2.3.1, p. 421 de [10] au couple (U, U_1), la suite (2.3.1) de [10] étant ici la suite $1 \to T \to R_{K/k}\mathbf{G}_m \to \mathbf{G}_m \to 1$ définie par la norme de K à k, on voit que la restriction du torseur Y^ξ au-dessus de U_1 est donnée par une équation

$$t^s(1-t)^r = \gamma.N_{K/k}(y_1\omega_1 + \cdots + y_n\omega_n) \neq 0,$$

où $\gamma \in k^*$ est un relèvement de $\xi \in k^*/N_{K/k}(K^*)$.

Puisque a et b sont premiers entre eux, il existe des entiers $r, s \in \mathbf{Z}$ tels que $ra - sb = 1$. Appliquons les considérations ci-dessus à la paire (r, s).

La restriction de Y^ξ à U_1 est donnée, comme k-variété, par le système d'équations :

$$t^s(1-t)^r = \gamma.N_{K/k}(y_1\omega_1 + \cdots + y_n\omega_n) \neq 0,$$

$$t^a(1-t)^b = \varepsilon.N_{K/k}(x_1\omega_1 + \cdots + x_n\omega_n) \neq 0.$$

Cette k-variété est k-isomorphe à la k-variété Z définie par

$$t = \varepsilon^r.\gamma^{-b}.N_{K/k}(u_1\omega_1 + \cdots + u_n\omega_n) \neq 0,$$

$$1-t = \gamma^a.\varepsilon^{-s}.N_{K/k}(v_1\omega_1 + \cdots + v_n\omega_n) \neq 0,$$

comme on voit par le changement de variables inversible :

$$u_1\omega_1 + \cdots + u_n\omega_n = (x_1\omega_1 + \cdots + x_n\omega_n)^r.(y_1\omega_1 + \cdots + y_n\omega_n)^{-b},$$

$$v_1\omega_1 + \cdots + v_n\omega_n = (y_1\omega_1 + \cdots + y_n\omega_n)^a.(x_1\omega_1 + \cdots + x_n\omega_n)^{-s}.$$

La k-variété Z est un ouvert lisse de l'hypersurface de l'espace affine $\mathbf{A}^{2n}$ d'équation

$$1 = \varepsilon^r.\gamma^{-b}.N_{K/k}(u_1\omega_1 + \cdots + u_n\omega_n) + \gamma^a.\varepsilon^{-s}.N_{K/k}(v_1\omega_1 + \cdots + v_n\omega_n).$$

La k-variété Z possède des points P'_v pour $v \in S$ correspondant par l'isomorphisme ci-dessus aux points P_v. Par ailleurs, comme la k-variété lisse Y^ξ possède des k_v-points pour toute place v, il en est de même de son ouvert défini par $t(1-t) \neq 0$, ce qui implique que la k-variété (lisse) Z a elle aussi des points dans tous les complétés de k.

Les arguments utilisés jusqu'ici valent sur tout corps de nombres. Pour conclure on utilise le théorème suivant, établi par la méthode du cercle par Heath-Brown et Skorobogatov (sur le modèle d'un travail beaucoup antérieur de Birch, Davenport et Lewis) : *Pour $k = \mathbf{Q}$, $\alpha, \beta, \gamma \in k^*$ et K/k une extension finie de corps de degré n, le principe de Hasse et l'approximation faible valent pour l'ouvert de lissité de l'hypersurface projective d'équation*

$$\alpha.w^n + \beta.N_{K/k}(u_1\omega_1 + \cdots + u_n\omega_n) + \gamma.N_{K/k}(v_1\omega_1 + \cdots + v_n\omega_n) = 0.$$

(Une telle démonstration, par la méthode du cercle, établit un résultat plus fort, elle donne une estimation du nombre de points de hauteur au plus B, pour B tendant vers l'infini.)

Dans le cas particulier $a = b = 1$ et K/k de degré 3, étudié dans [9], l'idée de combiner descente et méthode du cercle avait été suggérée par P. Salberger.

Le résultat obtenu ci-dessus suppose a et b premiers entre eux. Voici un cas où cette hypothèse n'est pas requise.

Théorème 1.8 *Soit K/k une extension finie de corps de nombres, et soit $\omega_1, \cdots, \omega_n$ une base de K/k. Soient a, b des entiers strictement positifs, non nécessairement premiers entre eux, et soit $\varepsilon \in k^*$. Soit U l'ouvert de lissité de la k-variété affine définie par l'équation*

$$t^a(1-t)^b = \varepsilon.N_{K/k}(x_1\omega_1 + \cdots + x_n\omega_n).$$

Soit X une k-compactification lisse de U.

Supposons que le corps k est le corps $\mathbf{Q}$ des rationnels, et que les espaces homogènes principaux sous le tore $R^1_{K/k}\mathbf{G}_m$ satisfont le principe de Hasse et l'approximation faible (c'est le cas par exemple si K/k est une extension cyclique ou si K/k est de degré premier).

Alors l'ensemble $X(k)$ est dense dans $X(\mathbf{A}_k)^{\mathrm{Br}(X)}$. L'adhérence de $X(k)$ dans $X(\mathbf{A}_k)$ est ouverte. L'approximation faible-faible vaut pour X.

Démonstration Comme on l'a observé ci-dessus, les fonctions t et $1-t$ ont un diviseur qui est une norme de diviseur sur U_K. Soit ici T le k-tore $(R^1_{K/k}\mathbf{G}_m)^2$. Comme ci-dessus, le torseur sous ce k-tore T défini sur l'ouvert $t(1-t)\neq 0$ de U par l'équation

$$t = N_{K/k}(y_1\omega_1+\cdots+y_n\omega_n),\ 1-t = N_{K/k}(z_1\omega_1+\cdots+z_n\omega_n)$$

s'étend en un torseur sur U sous T. On applique alors le théorème 1.6.

Un changement de variables simple montre que l'on obtient le produit d'une k-variété qui est un espace principal homogène sous $R^1_{K/k}\mathbf{G}_m$ par une hypersurface d'équation

$$\alpha+\beta N_{K/k}(u_1\omega_1+\cdots+u_n\omega_n)+\gamma N_{K/k}(v_1\omega_1+\cdots+v_n\omega_n)=0.$$

Les hypothèses permettent de conclure.

Remarques

(i) Pour K/k cyclique, dans la situation des théorèmes 1.7 et 1.8, il existe des contre-exemples à l'approximation faible (D. Coray, voir [9], §8).

(ii) Pour K/k de degré 3, le théorème 1.8 vaut sur tout corps de nombres ([9]).

(iii) Je renvoie à [24] pour l'observation suivante : si a ou b ou $a+b$ est premier avec n, alors tout modèle projectif de la variété définie par $t^a(1-t)^b=\varepsilon.N_{K/k}(x_1\omega_1+\cdots+\omega_nx_n)$ possède un point k-rationnel, ce qui sous les hypothèses du théorème assure que les points k-rationnels sont (Zariski-)denses. L'existence d'un k-point n'est pas garantie si par exemple $a=2, b=3, n=30$.

(iv) La validité du principe de Hasse et de l'approximation faible pour l'ouvert de lissité de l'hypersurface projective d'équation

$$\alpha.w^n+\beta.N_{K/k}(u_1\omega_1+\cdots+u_n\omega_n)+\gamma.N_{K/k}(v_1\omega_1+\cdots+v_n\omega_n)=0,$$

pour $k=\mathbf{Q}$, incite à penser que sur tout corps k, pour tout modèle projectif et lisse Z/k de cette hypersurface, le quotient $\mathrm{Br}(Z)/\mathrm{Br}(k)$ est trivial.

(v) Dans certains cas, on n'a pas besoin de recourir à la "descente ouverte". Ainsi pour la variété d'équation affine $t(1-t)=\varepsilon.N_{K/k}(x_1\omega_1+\cdots+x_n\omega_n)$, lorsque le degré de K/k est impair, le diviseur de t sur tout modèle projectif et lisse est une norme de l'extension K/k. On peut donc partir d'un torseur sous $R^1_{K/k}\mathbf{G}_m$ sur un modèle projectif et lisse.

(vi) Dans la situation des théorèmes 1.7 et 1.8, on peut prendre pour X une k-variété projective et lisse équipée d'un k-morphisme dominant $p: X\to\mathbf{P}^1_k$ étendant la projection $U\to\mathbf{A}^1_k=\mathrm{Spec}(k[t])$ définie par $(t,x_1,\cdots,x_n)\mapsto t$. L'invariant δ de cette fibration, comme défini dans l'introduction est en général 3 (fibres en $t=0,1,\infty$). En outre, pour le théorème 1.7, on ne suppose pas la validité du principe de Hasse dans les fibres (mais l'on sait que l'obstruction de Brauer-Manin est la seule pour les fibres). On comparera ce résultat avec ceux rappelés à la fin de l'introduction.

(vii) Une discussion lors du colloque de Budapest a permis, au prix d'un travail plus conséquent, de montrer que le théorème 1.7 vaut sans supposer que a et b sont premiers entre eux. Ceci fera l'objet d'une publication séparée ([6]). Une idée-clef est de faire une descente ouverte sur une k-variété lisse ouverte contenant strictement U, et contrôlable.

Chapitre 2 : Pinceaux d'espaces homogènes de variétés abéliennes

Revenons à la situation générale évoquée à la fin de l'introduction. Soient donc k un corps de nombres et $p: X\to\mathbf{P}^1_k$ un morphisme dominant de k-variétés lisses géométriquement intègres. Notons $K=k(\mathbf{P}^1_k)$. Soit X_η/K la fibre générique (lisse) de ce morphisme, supposée géométriquement connexe. Supposons que pour tout point fermé $M \in \mathbf{P}^1_k$ la fibre $X_M/k(M)$ possède une composante Y de multiplicité un telle que la clôture intégrale de $k(M)$ dans le corps des fonctions de Y est une extension abélienne de $k(M)$. Sous l'hypothèse de Schinzel, la condition $X(\mathbf{A}_k)^{\mathrm{Br}_{vert}} \neq \emptyset$ suffit à assurer l'existence de k-points $P \in \mathbf{P}^1(k)$ tels que la fibre X_P satisfasse $X_P(\mathbf{A}_k) \neq \emptyset$ (théorème 0.2). Lorsque le principe de Hasse vaut pour les fibres, ceci permet de conclure à l'existence de points k-rationnels sur X.

Dans ce chapitre, nous allons considérer le cas où la fibre générique X_η est un espace principal homogène sous une K-variété abélienne A_η, par exemple le cas où X_η est une courbe de genre un. Pour presque tout $P \in \mathbf{P}^1(k)$, la fibre X_P est un espace principal homogène sous la k-variété abélienne spécialisée A_P. Il est bien connu que le principe de Hasse ne vaut en général pas pour les espaces homogènes principaux de variétés abéliennes : sauf *heureux accident*, il n'y a pas de raison qu'une fibre X_P, qui possède des points dans tous les complétés de k, possède un point k-rationnel (on peut même donner des contre-exemples en famille [8]).

Depuis 1994, Swinnerton-Dyer et ses collaborateurs ont développé une technique qui permet précisément de forcer d'*heureux accidents* ([35], [14], [37], [2], [5], [39]).

Avant de décrire cette technique, il convient de rappeler ce qu'est le groupe de Tate-Shafarevich et ce qu'est le calcul de Selmer.

Rappels sur les groupes de Selmer

On se limite ici au cas de la multiplication par un nombre premier l sur une courbe elliptique E. Pour tout groupe abélien A et tout entier $n > 0$ on note ${}_nA$ le sous-groupe de A formé des éléments annulés par n. Cette notation sera aussi utilisée pour les schémas en groupes abéliens. De la suite de Kummer

$$0 \to {}_lE \to E \xrightarrow{x \mapsto lx} E \to 0,$$

on tire la suite exacte courte

$$0 \to E(k)/l \to H^1(k, {}_lE) \to {}_lH^1(k, E) \to 0.$$

Le groupe $H^1(k, E)$ classifie les espaces homogènes principaux sous E. Le groupe $H^1(k, {}_lE)$ classifie les l-revêtements de E, c'est-à-dire les torseurs $C \to E$, de groupe structural ${}_lE$, qui sur la clôture algébrique de k sont isomorphes au torseur $E \to E$ donné par la multiplication par l. L'espace total C d'un l-revêtement possède un k-point si et seulement s'il a une image triviale dans $H^1(k, E)$, si et seulement si sa classe dans $H^1(k, {}_lE)$ est dans l'image de $E(k)/l$.

On envoie ensuite la suite exacte

$$0 \to E(k)/l \to H^1(k, {}_lE) \to {}_lH^1(k, E) \to 0$$

dans le produit des suites exactes correspondantes sur chacun des complétés k_v :

$$0 \to \prod_v E(k_v)/l \to \prod_v H^1(k_v, {}_lE) \to \prod_v {}_lH^1(k_v, E) \to 0.$$

Le groupe de Tate-Shafarevich d'une k-variété abélienne A est par définition le noyau de l'application diagonale $H^1(k, A) \to \prod_v H^1(k_v, A)$. Ce groupe classifie les espaces homogènes principaux sous A qui ont des points dans chaque complété k_v. On a la conjecture bien connue :

Conjecture (Tate-Shafarevich) Pour toute variété abélienne A sur un corps de nombres k, le groupe de Tate-Shafarevich de A est un groupe fini.

On a la suite exacte naturelle

$$0 \to E(k)/l \to Sel_l(E) \to {}_l\text{Ш}^1(k, E) \to 0$$

obtenue à partir de la suite de Kummer par image réciproque via l'inclusion ${}_l\text{Ш}^1(k,E) \subset {}_lH^1(k,E)$. Le groupe de Selmer $Sel_l(E)$ classifie les l-revêtements $C \to E$ dont l'espace total C possède des points dans tous les complétés k_v. L'image de $E(k)/l$ dans $Sel_l(E)$ correspond exactement à ceux de ces revêtements $C \to E$ tels que $C(k) \neq \emptyset$. Ainsi la validité du principe de Hasse pour toutes les courbes C qui sont des l-revêtements de E équivaut à ${}_l\text{Ш}^1(k,E) = 0$.

Le groupe de Selmer est fini (alors que le groupe $H^1(k, {}_lE)$ est infini). Plus précisément, soit S un ensemble fini de places contenant les places archimédiennes, les places l-adiques et les places non archimédiennes où la courbe E n'a pas bonne réduction. Soit O_S l'anneau des S-entiers de k, et soit $\mathcal{E}/O_S$ le O_S-schéma abélien de fibre générique E/k. Si v est une place hors de S, l'image de la flèche $E(k_v)/l \to H^1(k_v, {}_lE)$ est le sous-groupe $H^1_{\text{ét}}(O_v, {}_l\mathcal{E}) \subset H^1(k_v, {}_lE)$. Ainsi $Sel_l(E)$ est contenu dans le sous-groupe de $H^1(k, {}_lE)$ formé des éléments non ramifiés en dehors de S, et ce groupe est fini ([31], II.6.2 Thm. 7 p. 117). Ledit sous-groupe s'identifie de fait au sous-groupe fini $H^1_{\text{ét}}(O_S, {}_l\mathcal{E}) \subset H^1(k, {}_lE)$ (c'est le principe de la démonstration du théorème de Mordell-Weil faible).

Pour une place v quelconque, on peut donner une caractérisation de l'image de $E(k_v)$ dans $H^1(k_v, {}_lE)$. On dispose de l'accouplement, symplectique et non dégénéré, de Weil

$${}_lE \times {}_lE \to \mu_l.$$

(Pour une variété abélienne, il faudrait ici faire intervenir la variété duale.) Pour tout place v de k, cet accouplement induit un accouplement, symplectique et non dégénéré, de groupes finis

$$H^1(k_v, {}_lE) \times H^1(k_v, {}_lE) \to H^2(k_v, \mu_l) \subset \mathbf{Z}/l.$$

(La dernière inclusion est fournie par le corps de classes local; pour v non archimédienne, c'est une égalité.)

Un résultat de Cassels, généralisé aux variétés abéliennes par Tate, assure que l'image de $E(k_v)/l$ dans $H^1(k_v, {}_lE)$ est un sous-espace isotrope maximal pour cet accouplement.

Soit $V_S = \oplus_{v \in S} H^1(k_v, {}_lE)$. Définissons sur V_S un accouplement symplectique et non dégénéré par somme orthogonale des accouplements précédents. On dispose du sous-groupe isotrope maximal $\oplus_{v \in S} E(k_v)/l \subset V_S$. On a par ailleurs la flèche composée $H^1(O_S, {}_l\mathcal{E}) \to H^1(k, {}_lE) \to V_S$, la dernière flèche étant la flèche diagonale. La loi de réciprocité assure que l'image de $H^1(O_S, {}_l\mathcal{E})$ est isotrope dans V_S.

Fixons un ensemble fini S_0 de places du corps de nombres k contenant toutes les places archimédiennes, toutes les places l-adiques, et tel que le groupe des classes de l'anneau O_{S_0} soit trivial. Des arguments classiques de théorie des nombres donnent le résultat suivant ([14], Prop. 1.2.1).

Proposition 2.1 *Supposons que tous les points d'ordre l de la courbe elliptique E sont rationnels sur k (ce qui implique que le corps k contient toutes les racines l-ièmes de l'unité). Pour tout ensemble fini S de places contenant S_0 et les places de mauvaise réduction de E, l'application de $H^1(O_S, {}_l\mathcal{E})$ dans V_S est injective, son image I^S est un sous-groupe isotrope maximal, et le groupe de Selmer $Sel_l(E)$ s'identifie au sous-groupe de $H^1(O_S, {}_l\mathcal{E}) \subset V_S$ orthogonal au sous-groupe isotrope maximal $\oplus_{v \in S} E(k_v)/l \subset V_S$.*

On voit donc que dans ce cas le groupe de Selmer est le noyau à droite de l'accouplement

$$\oplus_{v \in S} E(k_v)/l \times H^1(O_S, {}_l\mathcal{E}) \to \mathbf{Z}/l$$

obtenu par restriction de l'accouplement $V_S \times V_S \to \mathbf{Z}/l$. Le rang du groupe de Selmer $Sel_l(E)$ (comme $\mathbf{F}_l$-vectoriel) peut donc être calculé comme le corang d'une matrice *carrée* sur le corps $\mathbf{F}_l$.

Notons que, comme E a tous ses points d'ordre l rationnels sur k, on dispose d'éléments évidents dans $E(k_v)/l$, à savoir l'image du sous-groupe ${}_lE(k_v)$ (isomorphe à $(\mathbf{Z}/l)^2$) dans $E(k_v)/l$. Ces éléments sont fort utiles pour montrer que certaines classes dans $H^1(O_S, {}_lE)$ ne sont pas dans le groupe de Selmer.

La symétrisation du calcul de Selmer

Conservons l'hypothèse que le groupe ${}_lE$ est isomorphe au groupe constant $(\mathbf{Z}/l)^2$, ce qui pour S comme ci-dessus implique l'existence d'un isomorphisme de ${}_l\mathcal{E}$ avec le O_S-groupe constant $(\mathbf{Z}/l)^2$. Dans [35] sous une forme primitive, puis dans [14] de façon systématique, on a décrit un processus plus élaboré pour calculer le groupe de Selmer, au moyen d'une matrice carré plus petite que celle évoquée ci-dessus, et qui de plus possède la propriété étonnante d'être symétrique.

Le point de départ est un lemme général sur les sous-espaces maximaux isotropes d'une somme directe d'espaces symplectiques ([14], Lemma 1.1.3). Ce lemme montre qu'il existe des espaces isotropes maximaux $K_v \subset H^1(k_v, {}_lE)$ tels que $K_S = \oplus_{v \in S} K_v$ soit un supplémentaire de $H^1(O_S, {}_l\mathcal{E})$ dans V_S. De plus, pour $v \notin S_0$, on peut prendre, et on prendra $K_v = H^1(O_v, (\mathbf{Z}/l)^2)$.

On projette alors V_S vers $I^S \simeq H^1(O_S, {}_l\mathcal{E})$ le long de $\oplus_{v \in S} K_v$. L'accouplement ci-dessus induit un accouplement entre les $\mathbf{F}_l$-vectoriels $\mathbf{I}^S = I^S \cap (W^S + K_S)$ et $\mathbf{W}_S = W_S/(W_S \cap K_S) = \oplus_{v \in S} W_v/(W_v \cap K_v)$. On montre :

(i) La projection $V_S \to I^S$ induit par restriction à W_S un isomorphisme $\tau : \mathbf{W}_S \simeq \mathbf{I}^S$.

(ii) Le noyau de l'accouplement $\mathbf{I}^S \times \mathbf{W}_S \to \mathbf{Z}/l$ (à gauche ou à droite) est isomorphe à $Sel_l(E)$.

(iii) Via l'isomorphisme τ, cet accouplement définit une forme bilinéaire symétrique sur $\mathbf{W}_S$, et aussi sur $\mathbf{I}^S$.

Un principe de Hasse pour certains espaces homogènes principaux de variétés abéliennes

Comme remarqué par Manin ([26]), la finitude des groupes de Tate-Shafarevich implique que l'obstruction de Brauer-Manin au principe de Hasse pour les espaces homogènes principaux de variétés abéliennes est la seule obstruction. Nous ne nous servirons ici que d'une variante particulière de ce fait.

Proposition 2.2 *Soient k un corps de nombres et E/k une courbe elliptique. Soit l un nombre premier. Supposons la partie l-primaire du groupe Ш(E) finie. Si la dimension (sur $\mathbf{F}_l = \mathbf{Z}/l$) du sous-groupe de l-torsion de Ш(E) est au plus égale à 1, alors le sous-groupe de torsion l-primaire de E est trivial : si un espace principal homogène sous E est d'ordre une puissance de l, et s'il a des points dans tous les complétés de k, alors il a un point dans k.*

Démonstration Sous l'hypothèse que la torsion l-primaire Ш$(E)\{l\}$ est finie, Cassels a établi l'existence d'une forme alternée non dégénérée sur Ш$(E)\{l\}$. Ce groupe est donc une somme de groupes de type $(\mathbf{Z}/l^r)^2$. Sa l-torsion est donc une somme d'exemplaires de $(\mathbf{Z}/l)^2$, sa dimension sur $\mathbf{F}_l$ est paire. Le résultat suit (voir les rappels sur le groupe de Selmer).

Remarques

(i) On peut donner une généralisation aux variétés abéliennes principalement polarisées, en faisant attention au cas $l = 2$ (exemples de Poonen et Stoll).

(ii) On trouvera dans [2] et [5] une variante de cet énoncé dans le cas d'une isogénie de degré 2 (plutôt que la multiplication par 2), et une variante délicate dans le cas d'une isogénie de degré 3 dans [1] et [39].

(iv) En pratique, c'est le $\mathbf{F}_l$-rang d'un groupe de Selmer que l'on bornera. Par exemple, si la courbe elliptique E a tous ses points d'ordre l rationnels sur k, si l'application ${}_lE(k) \to E(k)/l$

est injective (cette condition est facile à assurer), et si le l-groupe de Selmer $Sel_l(E)$ est de dimension 3 sur $\mathbf{F}_l$, alors le rang de la courbe E sur k est un et tout l-revêtement de E qui a des points partout localement possède une infinité de points dans k.

A la recherche des points rationnels dans les fibres

Revenons à la situation d'une fibration $p : X \to \mathbf{P}^1_k$ satisfaisant les hypothèses générales mentionnées au début du chapitre. On fait les hypothèses suivantes :

(a) La fibre générique X_η est une courbe de genre un sur le corps $K = k(\mathbf{P}^1)$, et X_η ne possède pas de K-point.

(b) Il existe un premier l tel que la jacobienne E_η de X_η ait toute sa l-torsion rationnelle sur K, i.e. il existe un isomorphisme $(\mathbf{Z}/l)^2 \simeq {}_lE_\eta$.

(c) L'espace principal homogène non trivial X_η a une classe annulée par l dans $H^1(K, E_\eta)$, donc peut être représenté par un l-revêtement $X_\eta \to E_\eta$.

(d) On a $X(\mathbf{A}_k)^{\mathrm{Br}_{vert}} \neq \emptyset$.

Sous l'hypothèse de Schinzel, on trouve alors une infinité de points $P \in \mathbf{P}^1(k)$ tels que la fibre X_P soit lisse et ait des points dans tous les complétés de k (Théorème 0.2). Sauf cas très particulier le groupe de Selmer $Sel_l(E_P)$, qui est un $\mathbf{F}_l$-vectoriel, contient un sous-espace vectoriel de dimension 3, noté U_P, engendré par l'image de ${}_lE_P(k) \simeq (\mathbf{Z}/l)^2$ (l'application ${}_lE_P(k) \to E_P(k)/lE_P(k)$ étant injective si $E_P(k)$ n'a pas de point de l^2-torsion non de l-torsion) et par la classe du l-revêtement $X_P \to E_P$.

Si la dimension de $Sel_l(E_P)$ est 3, alors la dimension de ${}_l\text{Ш}(E_P)$ est au plus 1. La proposition 2.2 permet de conclure que ${}_l\text{Ш}(E_P) = 0$, que X_P possède un k-point, donc est isomorphe à E_P. En général, ceci montre aussi que la courbe E_P a un rang de Mordell-Weil égal à 1, et donc $X_P(k)$ est infini.

De façon générale, on cherche à montrer l'existence d'une infinité de points rationnels Q, "modifications" du point P, tels que l'on ait encore $X_Q(\mathbf{A}_k) \neq \emptyset$ mais tels que la dimension de $Sel_l(E_Q)$ soit 3. On peut alors conclure que $X(k)$ est dense pour la topologie de Zariski sur X.

On ne peut pas toujours garantir l'existence de tels points Q. Par exemple, si le rang de la partie libre du groupe $E_\eta(K)$ est au moins égal à 2, alors pour presque tout $Q \in \mathbf{P}^1(k)$, le rang de $Sel_l(E_Q)$ sur $\mathbf{F}_l$ est au moins 4.

On cherche à donner des conditions suffisantes contrôlables sur $X/\mathbf{P}^1_k$ permettant de trouver de tels points Q.

Il faut déjà pouvoir comparer les groupes de Selmer $Sel_l(E_P) \subset H^1(k, {}_lE_P)$ et $Sel_l(E_Q) \subset H^1(k, {}_lE_Q)$. C'est ici qu'intervient de façon essentielle l'hypothèse que la l-torsion de la fibre générique E_η est "constante" (hypothèse (b)). On a une identification naturelle de $(\mathbf{Z}/l)^2$ avec ${}_lE_P$ et ${}_lE_Q$. On peut donc voir les deux groupes de Selmer comme plongés dans le même espace $H^1(k, (\mathbf{Z}/l)^2)$.

Le groupe $Sel_l(E_P)$ est un sous-groupe du groupe fini $H^1(O_{S(P)}, (\mathbf{Z}/l)^2) \subset H^1(k, (\mathbf{Z}/l)^2)$, où $S(P)$ est un ensemble fini de places contenant la réunion des places de S_0 et des places où la courbe E_P a mauvaise réduction.

Commençons par préciser la définition de $S(P)$. On peut supposer la fibre à l'infini de $p : X \to \mathbf{P}^1_k$ lisse. Soit $\mathbf{A}^1_k = \mathrm{Spec}(k[t])$ le complémentaire du point à l'infini, et soient $R_i(t) \in k[t]$ les polynômes unitaires irréductibles définissant les points fermés $M \in \mathbf{A}^1_k$ avec mauvaise fibre (pas de composante de multiplicité un géométriquement intègre sur $k(M)$). Soit S_1 un ensemble fini de places contenant l'ensemble S_0 (donc les places archimédiennes et les places au-dessus de l), les places où l'un des polynômes $R_i(t)$ n'est pas entier, les places telles que chaque $R_i(t)$ est entier mais le produit $\prod_i R_i(t)$ ne se réduit pas en un polynôme séparable, et les places restantes où la fibration $X \to \mathbf{P}^1_k$ a mauvaise réduction. Pour $P \in \mathbf{A}^1(k)$ donné par $t = \lambda \in k$, à fibre X_P lisse, les places $v \notin S_1$ où la jacobienne E_P a mauvaise réduction sont parmi les places v telles que $v(R_i(\lambda)) \neq 0$ pour au moins un i. Pour le calcul du groupe de Selmer de E_P, on prendra $S(P)$ égal à la réunion des places dans S_1 et des places v telles que l'un des $v(R_i(\lambda)) \neq 0$.

On cherche un nouveau point Q très proche de P pour la topologie v-adique en toutes les places de $S(P)$. Si $\lambda_0 \in k$ est le paramètre de P, on cherche $\lambda \in k$ très proche de λ_0 aux places $v \in S(P)$. La nouvelle courbe E_Q est alors isomorphe à E_P sur chaque complété k_v pour $v \in S(P)$. On peut supposer $S(P) \subset S(Q)$ donc $H^1(O_{S(P)}, (\mathbf{Z}/l)^2) \subset H^1(O_{S(Q)}, (\mathbf{Z}/l)^2)$.

Soit $Z_P \subset Sel_l(E_P) \subset H^1(O_{S(P)}, (\mathbf{Z}/l)^2)$ un complémentaire du vectoriel U_P. On cherche Q (proche de P aux places dans $S(P)$) tel que l'image de Z_P dans $H^1(O_{S(Q)}, (\mathbf{Z}/l)^2)$ ait une intersection nulle avec $Sel(E_Q)$. Pour éliminer un élément non nul $\alpha \in Z_P$ par ce procédé, on cherche une place v non dans $S(P)$ et $Q \in \mathbf{P}^1(k)$ tels que α ne soit pas dans le noyau de l'accouplement

$$\oplus_{v \in S(Q) \setminus S(P)} \ {}_lE_Q(k_v) \ \times \ Z_P \to \ \mathbf{Z}/l$$

induit par

$$\oplus_{v \in S(Q)} \ E_Q(k_v)/l \ \times \ H^1(O_{S(Q)}, (\mathbf{Z}/l)^2) \to \ \mathbf{Z}/l.$$

Une telle place v si elle existe est à chercher parmi les v tels que l'un des $R_i(\lambda)$ ne soit pas une unité en v. En ce qui concerne le paramètre λ du point Q, la condition sera satisfaite pour tout Q dans un ouvert v-adique fixe.

On ne peut pas toujours trouver de tels v et Q, mais comme expliqué plus loin, on a su donner *des conditions suffisantes (conditions (Alg) ou (Arith) décrites ci-dessous)* le garantissant. Soit alors S_2 un ensemble de places v comme ci-dessus. Un argument simple montre qu'on peut trouver un ensemble de telles places, de cardinal exactement égal à la dimension de Z_P, et tel que l'accouplement

$$\oplus_{v \in S_2} \ {}_lE_Q(k_v) \ \times \ Z_P \to \ \mathbf{Z}/l$$

soit non dégénéré à droite.

Pour pouvoir contrôler le groupe de Selmer de E_Q, il ne faut pas que dans son calcul trop de nouvelles places apparaissent. Par ailleurs il faut aussi assurer $X_Q(\mathbf{A}_k) \neq \emptyset$.

Ici l'hypothèse de Schinzel joue à nouveau un rôle (rappelons qu'elle permet déjà d'établir l'existence d'un point P tel que $X_P(\mathbf{A}_k) \neq \emptyset$). Elle permet maintenant de trouver Q de paramètre λ proche de λ_0 aux places de $S(P) \cup S_2$, et tel que dans la décomposition de chaque $R_i(\lambda)$ il n'intervient outre les places précédentes qu'une seule nouvelle place v_i, où $R_i(\lambda)$ est une uniformisante. Soit S_3 la réunion des v_i. On peut alors calculer le groupe de Selmer de E_Q en se limitant aux places de $S(P) \cup S_2 \cup S_3$.

Tout ceci ne permet pas encore de trouver un groupe de Selmer de rang 3, en particulier parce que l'on ne voit pas comment contrôler l'accouplement

$$\oplus_{v \in S(Q)} E_Q(k_v)/l \times H^1(O_{S(Q)}, (\mathbf{Z}/l)^2) \to \mathbf{Z}/l$$

sur les éléments de $H^1(O_{S(Q)}, (\mathbf{Z}/l)^2)$ qui ne proviennent pas de $H^1(O_{S(P)}, (\mathbf{Z}/l)^2)$.

C'est ici qu'intervient la *symétrisation* du calcul de Selmer. Grâce à cette symétrisation, on peut "faire comme si" l'accouplement $\oplus_{v \in S} E_Q(k_v)/l \times H^1(O_{S(Q)}, (\mathbf{Z}/l)^2) \to \mathbf{Z}/l$ était donné par une forme bilinéaire symétrique $B_P : V_Q \times V_Q \to \mathbf{Z}/l$ (dans ce processus, on diminue la dimension des espaces concernés).

On décompose l'espace vectoriel V_P sous la forme $V_P = V_0 \oplus V_1 \oplus V_2$, où $V_0 \oplus V_1$ est le noyau de la forme bilinéaire B_P. La restriction de B_P à V_2 est non dégénérée. Le sous-vectoriel V_0, de dimension trois, est celui engendré par les points d'ordre l de E_P et la classe de X_P. En utilisant ce qui précède (et en particulier en utilisant l'hypothèse de Schinzel) on trouve un point Q tel que $V_Q = V_P \oplus V_3$, que la forme bilinéaire symétrique B_Q se restreigne sur V_P à la forme bilinéaire symétrique B_P, que la dimension de V_3 soit égale à la dimension de V_1, et que l'accouplement $B_Q : V_1 \times V_3$ soit non dégénéré. La *symétrie* de la forme bilinéaire B_Q implique alors que le noyau de la forme bilinéaire B_Q est réduit à V_0, donc le rang du groupe de Selmer de E_Q est trois.

Il nous reste à préciser les conditions suffisantes, mentionnées ci-dessus, qui permettent de réaliser ce programme. Elles sont en pratique performantes, mais sont difficiles à énoncer de façon formelle.

Le premier type de condition est de nature algébrique. On parlera ici d'une condition de type (Alg). C'est la "Condition (D)" apparaissant sous des formes diverses dans [35], [14], [37], [2], [5]. On demande qu'un certain sous-groupe d'un l-groupe de Selmer de nature algébrico-géométrique attaché à la fibre générique E_η soit aussi petit que possible, plus précisément qu'il soit de dimension 3 sur $\mathbf{F}_l$ (la condition impose en particulier automatiquement que le rang de la partie libre de $E_\eta(K)$ est au plus un) (pour cette interprétation de la "Condition (D)" en ces termes, voir [14], §4). Le l-groupe de Selmer classique (ci-dessus) est défini à partir d'une courbe elliptique E et des complétés k_v du corps de nombres k, ou encore de ses hensélisés. Le groupe de Selmer algébrico-géométrique défini dans [14] est associé à une courbe elliptique définie sur le corps $K = k(\mathbf{P}^1)$ et à l'ensemble des hensélisés stricts aux points fermés de $\mathbf{P}^1_k$ (la définition de ce groupe ne fait pas intervenir l'arithmétique du corps k). Le sous-groupe est défini au moyen d'applications associées aux fibres de mauvaise réduction de la famille de courbes sur $\mathbf{P}^1_k$. Si cette condition de type (Alg) est satisfaite, alors on arrive à éliminer le groupe Z_P. (Il y a là une analogie, a priori purement formelle, avec le théorème d'irréductibilité de Hilbert.)

Le second type de condition est arithmétique. On parlera ici d'une condition de type (Arith). C'est le type de condition imposé dans [39]. On demande a priori que pour chacune des classes non nulles (elles sont en nombre fini) dans Z_P il existe une place v (nécessairement non dans $S(P)$) telle que l'accouplement ${}_lE(k_v) \times H^1(k_v, (\mathbf{Z}/l)^2) \to \mathbf{Z}/l$ permette de l'éliminer. Cette description n'est qu'une approximation. La situation dans [39] est plus subtile : le nombre fini de classes "résistantes" dans $H^1(k, (\mathbf{Z}/l)^2)$ à prendre en compte ne dépend pas du point P trouvé initialement, il dépend seulement de la mauvaise réduction de la variété X. La condition imposée est qu'un certain nombre de variétés auxiliaires n'aient pas de points locaux.

Remarque Pour obtenir l'existence de points rationnels sur X, outre les conjectures de Schinzel et de Tate-Shafarevich, les hypothèses ont été :

(i) $X(\mathbf{A}_k)^{\mathrm{Br}_{vert}} \neq \emptyset$.

(ii) La condition (Alg) ; ou la condition (Arith).

On peut être surpris du résultat, qui semble ignorer la possibilité que le sous-ensemble $X(\mathbf{A}_k)^{\mathrm{Br}(X)} \subset X(\mathbf{A}_k)^{\mathrm{Br}_{vert}}$ soit vide.

En fait, dans le cas considéré dans [14], on montre (algébriquement, sans utiliser de conjectures) que la condition (Alg) est proche d'une autre condition : le sous-groupe l-primaire du groupe de Brauer de X coïncide avec celui de $\mathrm{Br}_{vert}(X/\mathbf{P}^1_k)$.

Dans la situation considérée dans [39], le groupe de Brauer n'est pas entièrement vertical, et la partie non verticale peut donner naissance à une obstruction au principe de Hasse. On peut vérifier (sans utiliser de conjectures) que la condition (Arith) imposée dans la preuve implique $X(\mathbf{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$.

En bref, pour chaque type de surface X discuté ci-après, les conditions qu'on est amené à imposer pour obtenir l'existence de points rationnels sont plus fortes que la simple condition $X(\mathbf{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$, hypothèse que nous ne savons pas utiliser directement, du moins en ce qui concerne la partie non verticale du groupe de Brauer.

Quelques résultats obtenus par cette méthode

Théorème 2.3 ([35]; [14] Prop. 3.2.1) *Soient k un corps de nombres et a_i, b_i, $i = 0, \cdots, 4$ des éléments de k^*. Soit $X \subset \mathbf{P}^4_k$ l'intersection de deux quadriques définie par*

$$\sum_{i=0}^{4} a_i T_i^2 = 0, \quad \sum_{i=0}^{4} b_i T_i^2 = 0.$$

Supposons :

(i) la torsion 2-primaire des groupes de Tate-Shafarevich des courbes elliptiques définies sur k est finie;

(ii) l'hypothèse de Schinzel est satisfaite.

Si les a_i, b_i sont suffisamment généraux, le principe de Hasse vaut pour X: si X a des points rationnels dans tous les complétés de k, alors X a des points k-rationnels.

(La condition précise sur les a_i, b_i est une condition d'indépendance sur les divers $d_{ij} = a_i b_j - a_j b_i$ ($i \neq j$) vus comme éléments de k^*/k^{*2}. Elle est satisfaite pour $a_0, \cdots, a_4, b_0, \ldots, b_4$ dans un ensemble de Hilbert de k^{10}.)

La démonstration de ce théorème utilise une fibration en courbes de genre un dont la fibre générique est un 2-revêtement d'une courbe elliptique dont tous les points d'ordre 2 sont rationnels. L'hypothèse que les a_i, b_i sont suffisamment généraux garantit d'une part que la condition (Alg) est satisfaite, d'autre part que la 2-torsion du groupe de Brauer vertical est triviale.

On trouvera dans [2] et [5] un résultat analogue pour des couples de formes quadratiques plus généraux (mais encore partiellement simultanément diagonales). On a une fibration analogue à celle évoquée ci-dessus, mais ici la courbe elliptique générique possède seulement un point de 2-torsion non trivial rationnel sur K.

Le dernier paragraphe de [2] laisse espérer la validité du théorème ci-dessus pour une intersection complète lisse de deux quadriques dans $\mathbf{P}^4_k$ sans aucune condition de diagonalisation simultanée (mais bien sûr avec des coefficients suffisamment généraux).

Dans [14], nous décrivons de nombreuses classes de surfaces fibrées en courbes de genre un pour lesquelles la méthode s'applique (le théorème ci-dessus apparaissant comme un cas très particulier). Une variante de [14] permet d'obtenir l'élégant résultat suivant.

Théorème 2.4 [37] *Soient $k = \mathbf{Q}$ et $a_i, i = 0, \cdots, 3$ des éléments de k^* dont le produit $a_0.a_1.a_2.a_3$ est un carré. Soit $X \subset \mathbf{P}^3_k$ 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 k est finie;

(ii) L'hypothèse de Schinzel est satisfaite.

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

(iv) L'ensemble $X(\mathbf{A}_k)^{\mathrm{Br}_1(X)}$ est non vide.

Alors X possède des points k-rationnels.

L'énoncé donné dans [37] n'est pas exactement formulé comme ci-dessus, mais un petit travail analogue à celui fait dans [5] devrait permettre de faire la traduction et d'étendre le résultat à tout corps de nombres.

La démonstration de ce théorème utilise une fibration en courbes de genre un dont la fibre générique est un 2-revêtement d'une courbe elliptique dont tous les points d'ordre 2 sont rationnels. L'hypothèse que les a_i sont suffisamment généraux garantit que la condition (Alg) est satisfaite.

La situation est donc tout à fait analogue à celle du théorème 2.3 et des résultats généraux de [14]. La différence dans l'exécution tient au fait suivant. Dans l'énoncé précis de la condition (Alg), la structure des fibres dégénérées (du modèle de Néron) de la fibration elliptique joue un rôle important. Ces fibres sont différentes dans les théorèmes 2.3 et 2.4.

Le théorème suivant a l'immense avantage de ne pas recourir à l'hypothèse de Schinzel.

Théorème 2.5 [39] *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.

Un argument relativement standard de fibration permet de déduire de ce théorème le corollaire spectaculaire suivant :

Théorème 2.6 [39] *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*

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

Rappelons qu'un tel énoncé est conjecturé pour toute hypersurface cubique lisse dans $\mathbf{P}^n_{\mathbf{Q}}$, $n \geq 4$, et que la méthode du cercle a permis de l'établir pour les hypersurfaces cubiques diagonales avec $n \geq 6$ (Davenport, 1959, pour $n \geq 8$; R. C. Baker, 1989, pour $n \geq 6$; pour $n \geq 7$, il existe toujours des solutions locales.)

On pourrait essayer de démontrer le théorème en prenant une droite rationnelle assez générale dans $\mathbf{P}^3_{\mathbf{Q}}$, et en considérant le pinceau de cubiques découpé sur la surface X par les plans passant par cette droite. Si le pinceau est assez général, toutes les courbes du pinceau sont géométriquement intègres – et on n'aurait pas alors besoin de recourir à l'hypothèse de Schinzel. Mais pour un pinceau général on n'espère pas trouver de sous-groupe "constant" $\mathbf{Z}/l \subset J_\eta$ dans la jacobienne de la courbe générique du pinceau.

Le point de départ de Swinnerton-Dyer est, après un changement de variable évident, d'écrire l'équation considérée sous la forme

$$a_0 T_0^3 + a_1 T_1^3 = a_2 T_2^3 + a_3 T_3^3.$$

(C'est aussi le point de départ de la démonstration par Hasse de son principe pour les formes quadratiques en 4 variables.) Plus précisément, on considère le cône affine Y dans $\mathbf{A}^4_{\mathbf{Q}}$ sur la surface X, défini par l'équation ci-dessus. Il suffit de trouver un $\mathbf{Q}$-point sur un modèle lisse de ce cône. Ce dernier est le produit fibré de deux courbes de genre un au-dessus de la droite $\mathbf{A}^1_{\mathbf{Q}} = \mathrm{Spec}(\mathbf{Q}[t])$:

$$a_0T_0^3 + a_1T_1^3 = t, \quad a_2T_2^3 + a_3T_3^3 = t.$$

Il existe un modèle projectif et lisse Z de Y équipé d'une fibration $p : Z \to \mathbf{P}^1_{\mathbf{Q}}$ étendant la projection $Y \to \mathbf{A}^1_{\mathbf{Q}}$ donnée par t. Pour tout point fermé M de $\mathbf{P}^1_{\mathbf{Q}}$ différent de $t = 0, \infty$, la fibre X_M possède une composante de multiplicité un géométriquement intègre. Ainsi $\delta(p) \leq 2$ et on peut appliquer le théorème 0.2 (a), qui recourt au théorème de Dirichlet mais pas à l'hypothèse de Schinzel générale.

L'autre aspect agréable de la fibration p est que la jacobienne de la fibre générique est le produit fibré des courbes elliptiques $T_0^3 + T_1^3 = a_0a_1tU^3$ et $T_2^3 + T_3^3 = a_2a_3tV^3$. Chacune de ces courbes possède un sous-groupe μ_3 constant. On peut donc espérer utiliser la méthode générale décrite plus haut.

Il ne semble pas y avoir dans le cas présent d'analogue de la condition (Alg) (comme les fibres de $Z \to \mathbf{P}^1_{\mathbf{Q}}$ sont de dimension plus grande que 1, on ne peut ici suivre l'analyse du §4 de [14]).

De façon un peu surprenante, le groupe de Brauer vertical associé à la situation est trivial (proposition 3.5 ci-après). Sous l'hypothèse que X, et donc Z, possède partout localement des points, le théorème 0.2 (a) permet de trouver des points $P \in \mathbf{P}^1(\mathbf{Q})$ tels que Z_P, qui est le produit de deux courbes de genre un, ait des points dans chacun des complétés. A chacune de ces deux courbes on associe un élément d'un groupe de Selmer convenable (associé à une isogénie de degré 3). On essaye de remplacer le point P par un autre point Q tel que la somme des dimensions (sur $\mathbf{F}_3$) des deux groupes de Selmer en ce point soit strictement plus petite. On a ici un analogue de la "symétrisation" du groupe de Selmer, mais le processus pour décroître l'ordre des deux groupes est extrêmement subtil. Ce processus bute à un certain moment. C'est ce qui amène à imposer la condition (Arith) mentionnée plus haut, qui est satisfaite sous les hypothèses (i) ou (ii) du théorème 2.5. On rencontre ici une difficulté supplémentaire lorsqu'on cherche à établir, pour les isogénies concernées, l'analogue de la proposition 2.2. Cette difficulté tient à l'existence de multiplication complexe par $\mathbf{Q}(\mu_3)$ sur les courbes considérées. Pour obtenir le substitut convenable, on utilise le fait que $\mathbf{Q}$ ne contient pas les racines cubiques de l'unité ! L'analogue des théorèmes 2.5 et 2.6 vaut d'ailleurs sur tout corps de nombres k tel que l'extension $k(\mu_3)/k$ est non triviale.

Remarque Soient $g_1(x)$ et $g_2(x)$ des polynômes séparables de degré 4 sur un corps de nombres k. Considérons la k-variété affine définie dans l'espace affine avec coordonnées t, x_1, x_2, y_1, y_2 par les équations

$$y_1^2 g_1(x_1) = t = y_2^2 g_2(x_2).$$

Cette variété est k-birationnelle au produit fibré, au-dessus de $\mathbf{A}^1_k = \mathrm{Spec}(k[t])$, des courbes de genre 1 d'équation affine $y_1^2 = tg_1(x_1)$ et $y_2^2 = tg_2(x_2)$. Chacune de ces courbes a bonne réduction en dehors de $t = 0, \infty$. La jacobienne de chacune de ces courbes est une courbe elliptique sur le corps $k(t)$ dont la 2-torsion est un $k(t)$-groupe qui provient d'un k-groupe. Si les résolvantes de g_1 et g_2 ont toutes leurs solutions dans k, ce k-groupe est $(\mathbf{Z}/2)^2$. On est donc dans une situation analogue à celle étudiée dans [39]. En outre, sauf pour des polynômes g_1 et g_2 très particuliers, on n'a pas la difficulté due à la multiplication complexe. On peut espérer dans une telle situation obtenir des résultats parallèles à ceux de [39].

Chapitre 3 : Surfaces et hypersurfaces cubiques diagonales sur un corps de fonctions

Dans ce chapitre, je montre que les résultats de l'article [39] de Swinnerton-Dyer, que l'on vient de discuter, et qui dépendent de la finitude de groupes de Tate-Shafarevich, admettent des analogues inconditionnels lorsque l'on remplace les corps de nombres par des corps globaux de caractéristique positive.

Quand on parle d'un corps de fonctions k sur un corps fini $\mathbf{F}_q$, on sous-entend que le corps $\mathbf{F}_q$ est algébriquement clos dans k. Ainsi la condition $q \equiv 2$ mod. 3 dans les énoncés suivants équivaut au fait que la caractéristique de k est différente de 3 et que le corps k ne contient pas les racines cubiques primitives de l'unité.

Théorème 3.1 *Soit k un corps de fonctions d'une variable sur un corps fini $\mathbf{F}_q$ avec q impair, $q \equiv 2$ mod. 3. Soient $a, b, c, d \in k^*$. Si la surface cubique V d'équation*

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

possède des points dans tous les complétés k_v de k, alors, sous chacune des hypothèses suivantes, elle possède un point dans k.

(i) Il existe des places v, w de k satisfaisant : $v(b), v(c), v(d), w(a), w(c), w(d)$ sont tous divisibles par 3, mais ni $v(a)$ ni $w(b)$ ne le sont.

(ii) Il existe une place v de k telle que $v(a)$ n'est pas divisible par 3 alors que $v(b), v(c), v(d)$ le sont, et l'un des quotients $b/c, c/d$ n'est pas un cube dans le complété k_v.

(iii) Il existe une place v de k telle que $v(c)$ et $v(d)$ sont divisibles par 3 alors que ni $v(a)$ ni $v(b)$ ne le sont, et la surface cubique $V \times_k k_v$ n'est pas birationnelle à un plan sur le corps k_v.

(Cette dernière condition peut s'exprimer de façon explicite en terme des coefficients.)

Théorème 3.2 *Soit k un corps de fonctions d'une variable sur un corps fini $\mathbf{F}_q$ avec q impair et $q \equiv 2$ mod. 3. Si une hypersurface cubique diagonale*

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

a des points rationnels dans tous les complétés de k, alors elle a des points dans k.

Le travail de Swinnerton-Dyer utilise un certain nombre de résultats qui pourraient a priori paraître spécifiques aux corps de nombres. Dans ce chapitre, qui renvoie constamment à l'article [39], on indique simplement les substituts nécessaires pour couvrir le cas des corps globaux de caractéristique positive. Certains des commentaires ont aussi leur intérêt dans le cas des corps de nombres. Le lecteur est donc supposé lire ce chapitre avec l'article [39] sous la main. Sauf mention contraire, les références dans ce chapitre sont aux lemmes, propositions, paragraphes etc. de [39].

La théorie du corps de classes pour les corps de fonctions d'une variable sur un corps fini est due à Hasse, F. K. Schmidt et Witt. Elle fut développée dans un cadre plus géométrique par Lang (voir le livre [29] de Serre). Le théorème de Tchebotarev dans le cas fonctionnel est établi par Lang [25] et Serre [30]. Voir en particulier le théorème 1, chap. VI, §16, p. 135 de [29].

On note $\mathbf{F}$ un corps fini de cardinal congru à 2 modulo 3, c'est-à-dire un corps fini qui ne contient pas de racine cubique non triviale de 1. On note $\mathbf{F}'$ le corps $\mathbf{F}[X]/(X^2 + X + 1)$. On considère une $\mathbf{F}$-courbe C, projective, lisse, géométriquement connexe. On note $k = \mathbf{F}(C)$ son corps des fonctions. On note $C' = C \times_{\mathbf{F}} \mathbf{F}'$ et $K = \mathbf{F}'(C')$ le corps des fonctions de C', corps qui est donc obtenu à partir de k par ajout des racines cubiques de 1 : c'est une extension "constante" du corps de fonctions d'une variable k. On note $G = \mathrm{Gal}(\mathbf{F}'/\mathbf{F}) = \mathrm{Gal}(K/k)$, et on note σ ($\sigma^2 = 1$) l'élément non trivial de G.

Etant donnés $a, b, c, d \in k^*$, on considère la surface cubique non singulière V/k définie par

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

On fixe un ensemble fini S_0 de places de K contenant un ensemble de générateurs du groupe de Picard $\mathrm{Pic}(C')$ (on rappelle que le sous-groupe $\mathrm{Pic}^0(C') \subset \mathrm{Pic}(C')$ des classes de degré zéro est le groupe des points rationnels d'une variété abélienne sur un corps fini, donc est fini), et on suppose S_0 stable par G. On note S_1 un ensemble fini de places de K, stable par G, contenant S_0 et contenant toutes les places v de K pour lesquelles l'un de $v(a), v(b), v(c), v(d)$ n'est pas divisible par 3.

Il n'y a rien à modifier à la description de la "première descente" sur une courbe $X^3 + Y^3 = AZ^3$ avec $A \in k^*$ au début du paragraphe 2.

Dans le cas fonctionnel, le paragraphe précédant le lemme 1 (voir formules (8)) est à remplacer par les considérations (plus simples) suivantes. On se donne un ensemble fini S de places (points fermés) de C', stable par σ. Soit n son ordre. On note $U' \subset C'$ l'ouvert complémentaire de S. On considère l'application naturelle de $\mathbf{Z}/3$-vectoriels

$$\varphi : \mathbf{F}'[U']^*/\mathbf{F}'[U']^{*3} \to \oplus_{v \in S} K_v^*/K_v^{*3}$$

induite par les inclusions $\mathbf{F}'[U'] \subset K \subset K_v$.

Fixons un isomorphisme $\mathbf{Z}/3 = \mu_3$ au-dessus de K. Le second espace vectoriel, qui par la théorie de Kummer s'identifie à $\oplus_{v \in S} H^1(K_v, \mu_3)$, est alors muni d'une structure naturelle d'espace alterné non dégénéré, donnée par la somme des cup-produits (symboles de Hilbert)

$$H^1(K_v, \mu_3) \times H^1(K_v, \mu_3) \to H^2(K_v, \mu_3^{\otimes 2}) = H^2(K_v, \mu_3) = \mathbf{Z}/3,$$

dont chacun est alterné non dégénéré ([31], II.5.8 Thm. 6 p. 112).

L'analogue du lemme de départ de [39] (remarques précédant le lemme 1) est ici :

Lemme 3.3 *Avec les notations ci-dessus,*
a) la dimension du $\mathbf{Z}/3$*-vectoriel* $\oplus_{v \in S} K_v^*/K_v^{*3}$ *est* $2n$*;*
b) l'application φ *a une image totalement isotrope;*
c) si de plus $\mathrm{Pic}(U') = 0$*, alors l'application* φ *est injective, et son image est un sous-espace totalement isotrope maximal de* $\oplus_{v \in S} K_v^*/K_v^{*3}$*.*

Démonstration Pour tout point fermé v de C', le complété K_v est isomorphe à $\mathbf{F}_v((t))$, où le corps résiduel $\mathbf{F}_v$ est un corps de caractéristique différente de 3 et contenant les racines cubiques de 1. Le quotient $\mathbf{F}_v^*/\mathbf{F}_v^{*3}$ est donc d'ordre 3, et le quotient K_v^*/K_v^{*3} isomorphe à $(\mathbf{Z}/3)^2$, ce qui établit le point a). Le point b) résulte par exemple de la loi de réciprocité pour le groupe de Brauer de $\mathbf{F}'(C)$. Pour le point c), la dualité de Poitou-Tate (Milne [27], I, Thm. 4.10 p. 70) montre que le noyau de φ s'identifie au dual du noyau de l'application

$$H^2_{\text{ét}}(U', \mathbf{Z}/3) \to \oplus_{v \in S} H^2(K_v, \mathbf{Z}/3).$$

Sous l'hypothèse $\mathrm{Pic}(U') = 0$, la suite de Kummer donne un isomorphisme $H^2_{\text{ét}}(U', \mu_3) \simeq {}_3\mathrm{Br}(U')$. Comme $\mathbf{Z}/3 \simeq \mu_3$ sur C', le noyau ci-dessus s'identifie donc au noyau de

$${}_3\mathrm{Br}(U') \to \prod_{v \in S} {}_3\mathrm{Br}(K_v),$$

c'est-à-dire, la courbe C' étant lisse, à un sous-groupe de ${}_3\mathrm{Br}(C')$. Et l'on sait ([16] III (2.15)) qu'une courbe projective lisse connexe sur un corps fini a un groupe de Brauer nul.

Pour établir que l'image de φ est un sous-espace totalement isotrope maximal, il suffit maintenant de montrer que la dimension du $\mathbf{Z}/3$-vectoriel $\mathbf{F}'[U']^*/\mathbf{F}'[U']^{*3}$ est n. Ceci s'établit simplement en considérant la multiplication par 3 sur la suite exacte

$$0 \to \mathbf{F}'[U']^*/\mathbf{F}'^* \to \oplus_{v\in S}\mathbf{Z} \to \mathrm{Pic}(C') \to 0$$

(l'exactitude à droite provient de l'hypothèse $\mathrm{Pic}(U') = 0$), en utilisant la finitude du noyau $\mathrm{Pic}^0(C')$ de l'application degré $\mathrm{Pic}(C') \to \mathbf{Z}$, et en tenant compte du fait déjà mentionné $F'^*/F'^{*3} \simeq \mathbf{Z}/3$.

Remarque Dans le cas fonctionnel, pour *toute* place v de K, notant O_v l'anneau des entiers du complété K_v, on voit que le quotient $T_v = O_v^*/O_v^{*3} \simeq \mathbf{Z}/3$ est un sous-espace isotrope maximal de $K_v^*/K_v^{*3} \simeq (\mathbf{Z}/3)^2$ (alors que pour les corps de nombres on doit faire attention aux places 3-adiques).

Le lemme 1 de [39] est un lemme d'algèbre linéaire abstrait, il est délicat mais ne requiert aucune modification dans notre contexte.

Les considérations suivant ce lemme valent encore, avec quelques simplifications. Pour E/k définie par une équation $X^3 + Y^3 = AT^3$ et v place de K, l'image W_v de l'application de Kummer $E(K_v) \to K_v^*/K_v^{*3} \simeq (\mathbf{Z}/3)^2$ est $T_v = O_v^*/O_v^{*3} \simeq \mathbf{Z}/3$ si $v(A)$ est divisible par 3, sinon c'est le groupe $\mathbf{Z}/3$ engendré par la classe de A dans K_v^*/K_v^{*3}.

Discutons maintenant le paragraphe précédant le lemme 2, et le groupe noté G_0 par Swinnerton-Dyer. Pour la commodité du lecteur, rappelons que la "norme absolue" n'est autre que le cardinal du corps résiduel. A toute place $v \in C$ on associe la classe de l'élément de Frobenius dans le groupe $\pi_1^{ab}(C)$, groupe de Galois de l'extension abélienne maximale non ramifiée de $k = \mathbf{F}(C)$. On obtient ainsi une application du groupe des diviseurs de C dans $\pi_1^{ab}(C)$, et cette application passe au quotient par l'équivalence rationnelle, définissant un homomorphisme $\mathrm{Pic}(C) \to \pi_1^{ab}(C)$. La flèche $\mathrm{Pic}(C) \to \mathbf{Z}$ définie par le degré sur $\mathbf{F}$ et la flèche $\pi_1^{ab}(C) \to \hat{\mathbf{Z}}$, où $\hat{\mathbf{Z}}$ est le groupe de Galois absolu de $\mathbf{F}$ et la seconde flèche est induite par la flèche structurale $C \to \mathrm{Spec}(\mathbf{F})$, sont compatibles. Le groupe $G_0 \subset \mathrm{Pic}(C)$ est le sous-groupe noyau de l'application composée $\mathrm{Pic}(C) \to \mathbf{Z} \to \mathbf{Z}/2$, une place $v \in C$ est dans le noyau de cette flèche si et seulement si le Frobenius F_v correspondant induit $1 \in \mathrm{Gal}(\mathbf{F}'/\mathbf{F})$.

Le début du lemme 2 est inchangé. On pourrait remplacer le quatrième paragraphe (commençant par "In this case I claim ...") par les considérations suivantes, aussi valables dans le cas des corps de nombres, dès que S contient les places au-dessus de 3, considérations qui n'utilisent pas l'hypothèse que le générateur σ de $\mathrm{Gal}(K/k)$ agit sans point fixe sur S. Soient $U = C \setminus S$ et $U' = U \times_{\mathbf{F}} \mathbf{F}'$. Le revêtement U'/U est galoisien, fini et étale de groupe G. La suite spectrale de Hochschild-Serre $E_2^{pq} = H^p(G, H^q_{\text{ét}}(U', \mu_3)) \implies H^n_{\text{ét}}(U, \mu_3)$ a tous ses termes avec $p > 0$ nuls, puisqu'annulés par 2 (ordre de G) et 3 (exposant de μ_3). Ainsi $H^1_{\text{ét}}(U, \mu_3) = H^1_{\text{ét}}(U', \mu_3)^G$. L'hypothèse que $\mathrm{Pic}(U') = 0$ implique que le groupe $\mathrm{Pic}(U) = H^1_{\text{ét}}(U, \mathbf{G}_m)$ est annulé par 2, en particulier n'a pas de 3-torsion. Les suites de cohomologie déduites de la suite de Kummer

$$1 \to \mu_3 \to \mathbf{G}_m \xrightarrow{x\mapsto x^3} \mathbf{G}_m \to 1$$

pour U, resp. U', donnent alors $\mathbf{F}[U]^*/\mathbf{F}[U]^{*3} = H^1_{\text{ét}}(U, \mu_3)$ et $\mathbf{F}'[U]^*/\mathbf{F}'[U]^{*3} = H^1_{\text{ét}}(U', \mu_3)$, isomorphismes compatibles aux flèches de restriction. On a donc

$$\mathbf{F}[U]^*/\mathbf{F}[U]^{*3} = (\mathbf{F}'[U]^*/\mathbf{F}'[U]^{*3})^G.$$

Remarque On pourrait donner une démonstration plus élémentaire en considérant la cohomologie de la suite exacte de G-modules

$$1 \to \mathbf{F}'[U]^* \to \mathbf{F}'(C)^* \to \mathrm{Div}(U') \to 0.$$

Un calcul un peu plus subtil, spécialement dans le cas des corps de nombres, est celui apparaissant au paragraphe suivant ("Denote the order ..."). Montrons que ce calcul, qui suppose que σ agit sans point fixe sur S, vaut aussi dans le cas des corps de fonctions. Soit $n = 2m$ l'ordre de S. On considère la suite exacte de G-modules

$$1 \to \mathbf{F}'[U]^*/\mathbf{F}'^* \to P \to \mathrm{Pic}(C') \to 0,$$

où $P = \oplus_{v\in S}\mathbf{Z}$ désigne le groupe des diviseurs de C' engendré par les places de S. Ce G-module est un module de permutation, en particulier $H^1(G, P) = 0$. C'est un groupe abélien libre de rang $n = 2m$, et l'hypothèse que σ agit sans point fixe sur S assure que le groupe P^G est libre de rang m. La suite exacte ci-dessus donne naissance à la suite exacte

$$1 \to (\mathbf{F}'[U]^*/\mathbf{F}'^*)^G \to P^G \to (\mathrm{Pic}(C'))^G \to H^1(G, \mathbf{F}'[U]^*/\mathbf{F}'^*) \to 0.$$

Comme on a $H^1(G, \mathbf{F}'^*) = 0$ (théorème 90 de Hilbert) et $H^2(G, \mathbf{F}'^*) = 0$ (trivialité du groupe de Brauer du corps fini $\mathbf{F}$), on peut réécrire cette suite exacte sous la forme

$$1 \to \mathbf{F}[U]^*/\mathbf{F}^* \to P^G \to \mathrm{Pic}(C) \to H^1(G, \mathbf{F}'[U]^*/\mathbf{F}'^*) \to 0.$$

En utilisant le fait que $H^1(G, \mathbf{F}'[U]^*/\mathbf{F}'^*)$ est annulé par 2, la considération de la multiplication par 3 sur cette suite et une chasse au diagramme facile donnent une suite exacte

$$0 \to {}_3\mathrm{Pic}(C) \to \mathbf{F}[U]^*/\mathbf{F}^*.\mathbf{F}[U]^{*3} \to P^G/3 \to \mathrm{Pic}(C)/3 \to 0.$$

Le groupe $\mathrm{Pic}(C)$ est une extension de $\mathbf{Z}$ par un groupe fini. De la suite ci-dessus on tire que la dimension du $\mathbf{Z}/3$-vectoriel $\mathbf{F}[U]^*/\mathbf{F}^*.\mathbf{F}[U]^{*3}$ est $m-1$. Comme $\mathbf{F}^*/\mathbf{F}^{*3}$ est d'ordre 1, on conclut que la dimension du $\mathbf{Z}/3$-vectoriel $\mathbf{F}[U]^*/\mathbf{F}[U]^{*3}$ est $m-1$.

Par ailleurs de la suite exacte

$$1 \to \mathbf{F}'[U]^*/\mathbf{F}'^* \to P \to \mathrm{Pic}(C') \to 0$$

on déduit que $\mathbf{F}'[U]^*/\mathbf{F}'^*$ est un groupe abélien libre de rang $2m-1$. Comme $\mathbf{F}'^*/\mathbf{F}'^{*3}$ est d'ordre 3, on voit que le $\mathbf{Z}/3$-vectoriel $\mathbf{F}'[U]^*/\mathbf{F}'[U]^{*3}$ a pour dimension $n = 2m$.

La situation est donc identique à celle décrite dans [39] (avec $X_S = \mathbf{F}'[U]^*/\mathbf{F}'[U]^{*3}$ et $X_\Sigma = \mathbf{F}[U]^*/\mathbf{F}[U]^{*3}$).

Il n'y a aucune modification à apporter à la fin du paragraphe 2 de [39].

Passons au paragraphe 3. L'énoncé à établir est le suivant.

Proposition 3.4 *Soit Σ un ensemble des places v de k contenant toutes les places v telles que l'un de $v(a), v(b), v(c), v(d)$ ne soit pas divisible par 3. Soit, pour chaque place dans Σ, un élément $\gamma_v \in k_v^*$ tel que le système*

$$ax^3 + by^3 = \gamma_v = cz^3 + dt^3$$

admette une solution dans k_v. Il existe alors $\gamma \in k^*$ tel que, pour toute place v de k, le système

$$ax^3 + by^3 = \gamma = cz^3 + dt^3$$

admette une solution dans k_v. On peut choisir γ tel que $\gamma/\gamma_v \in k_v^*$ soit un cube pour chaque place $v \in \Sigma$, et que le support du diviseur de γ soit formé de places de Σ et de places inertes dans K. Si de plus σ agit sans point fixe sur Σ, on peut faire en sorte que la partie première à Σ du diviseur de γ soit de la forme $2p + q + r$ avec p, q, r places de k (i.e. points fermés de la courbe C) inertes dans K, i.e. telles que le corps résiduel ait un ordre congru à 2 modulo 3.

Démonstration Par la théorie du corps de classes géométrique, le groupe I_k/k^* des classes d'idèles de k s'identifie au sous-groupe du groupe $\mathrm{Gal}(k^{ab}/k)^0$ du groupe de Galois $\mathrm{Gal}(k^{ab}/k)$ formé des classes qui induisent une puissance entière de l'élément de Frobenius dans le groupe de Galois absolu de $\mathbf{F}$. A un sous-groupe ouvert H_L de $\mathrm{Gal}(k^{ab}/k)^0$ correspond une extension abélienne finie L de k.

Par approximation faible, on trouve $\gamma_1 \in k^*$ tel que $\gamma_1/\gamma_v \in k_v^{*3}$ pour chaque $v \in \Sigma$. Ecrivons le diviseur de γ_1 sur C comme la somme d'un diviseur Δ à support dans Σ et d'un diviseur Δ_1 étranger à Σ:

$$\mathrm{div}_C(\gamma_1) = \Delta + \Delta_1.$$

Considérons le sous-groupe ouvert $W = \prod_{v \in \Sigma} k_v^{*6} \times \prod_{v \notin \Sigma} O_v^*$ de I_k, où $O_v^* \subset k_v^*$ désigne le sous-groupe des unités. Le sous-groupe $k^*.W \subset I_k$ est ouvert d'indice fini, la théorie du corps de classes définit un isomorphisme entre $I_k/k^*.W$ et le groupe de Galois $\mathrm{Gal}(L/k)$ d'une extension finie abélienne L de k contenant K/k (ce dernier point est assuré par le fait que l'on a pris des puissances sixièmes dans la définition de W). Au diviseur Δ_1 est associée une classe bien définie dans $I_k/k^*.W$. Soit τ son image dans $\mathrm{Gal}(L/k)$. L'image de τ dans $\mathrm{Gal}(K/k) \simeq \mathbf{Z}/2$ est la classe, dans $\mathbf{Z}/2$, du degré du diviseur Δ_1 de C (par rapport au corps $\mathbf{F}$).

Supposons d'abord que τ induise l'élément non trivial de $\mathrm{Gal}(K/k)$. Le théorème de Tchebotarev assure l'existence d'une place $v_1 \notin \Sigma$ dont l'élément de Frobenius associé dans $\mathrm{Gal}(L/k)$ est τ. La place v_1 est donc inerte dans l'extension K/k. Il existe un élément $\delta \in k^*$ et un diviseur Δ_2 à support dans Σ tels que

$$\mathrm{div}_C(\delta) = \Delta_1 - v_1 + \Delta_2$$

et que de plus $\delta \in k_v^{*6}$ pour $v \in \Sigma$. Soit $\gamma = \gamma_1/\delta$. On a donc

$$\mathrm{div}_C(\gamma_1/\delta) = v_1 + \Delta_3$$

avec Δ_3 à support dans Σ, et $v_1 \notin \Sigma$, v_1 inerte dans K. Par ailleurs $\gamma/\gamma_v = (\gamma_1/\gamma_v).(1/\delta) \in k_v^{*3}$ pour chaque place $v \in \Sigma$.

Si τ induit l'élément trivial de $\mathrm{Gal}(K/k)$, on choisit, ce qui est loisible par le théorème de Tchebotarev, une place $v_0 \notin \Sigma$ dont l'élément de Frobenius associé dans $\mathrm{Gal}(L/k)$ induise l'élément non trivial de $\mathrm{Gal}(K/k)$. Au diviseur $\Delta_1 + v_0$ est associé une classe bien définie dans $I_k/k^*.W$, dont l'image dans $\mathrm{Gal}(L/k)$ induit l'élément non trivial de $\mathrm{Gal}(K/k)$. Utilisant le théorème de Tchebotarev comme ci-dessus, on trouve une place $v_1 \notin \Sigma$ inerte dans K/k, distincte de v_0, un élément $\delta \in k^*$ et un diviseur Δ_2 à support dans Σ tels que

$$\mathrm{div}_C(\delta) = \Delta_1 - v_1 - v_0 + \Delta_2$$

et que de plus $\delta \in k_v^{*6}$ pour $v \in \Sigma$. Soit $\gamma = \gamma_1/\delta$. On a alors

$$\mathrm{div}_C(\gamma_1/\delta) = v_1 + v_0 + \Delta_3$$

avec Δ_3 à support dans Σ, et $v_0, v_1 \notin \Sigma$, $v_0 \neq v_1$ inertes dans K. Par ailleurs, pour chaque place $v \in \Sigma$, on a $\gamma/\gamma_v = (\gamma_1/\gamma_v).(1/\delta) \in k_v^{*3}$.

Dans l'un comme dans l'autre cas, l'équation

$$ax^3 + by^3 = \gamma = cz^3 + dt^3$$

a des solutions dans tous les complétés k_v. C'est clair pour les places $v \notin \Sigma \cup \{v_1\} \cup \{v_0\}$, tous les coefficients étant alors des unités (à des cubes près). Pour $v \in \Sigma$, c'est aussi clair d'après l'hypothèse, puisqu'on a $\gamma/\gamma_v \in k_v^{*3}$. Les places v_0 et v_1 sont inertes dans K/k, le corps résiduel en une telle place est un corps fini qui ne contient pas de racine cubique non triviale de l'unité, donc l'élévation au cube dans ce corps résiduel est une bijection, et toute unité dans k_v^* est un cube. Pour une telle place v, chacune des deux courbes cubiques lisses

$$ax^3 + by^3 = \gamma.u^3, \ cz^3 + dt^3 = \gamma.u^3$$

admet un point rationnel dans k_v avec $u = 0$, elle admet donc d'autres points avec $u \neq 0$, et le système

$$ax^3 + by^3 = \gamma = cz^3 + dt^3$$

admet une solution dans k_{v_0} et dans k_{v_1}.

La démonstration ci-dessus établit plus généralement le résultat suivant. Soient $v_1, \dots, v_n$ des places de k non dans Σ, et soient $r_1, \dots, r_n$ des entiers. Partant de γ_1 comme ci-dessus, on peut trouver $\gamma \in k^*$ tel que $\gamma/\gamma_v \in k_v^{*3}$ pour $v \in \Sigma$ et tel que la partie étrangère à Σ du diviseur de γ sur C soit de la forme $\sum_i r_i v_i + w_0 + \varepsilon w_1$ avec w_0 et w_1 inertes dans K, et $\varepsilon = 0$, resp. $\varepsilon = 1$, si le degré (sur $\mathbf{F}$) du diviseur $\Delta_1 + \sum_i r_i v_i$ est impair, resp. pair.

Le degré de $\mathrm{div}_C(\gamma_1) = \Delta + \Delta_1$ est nul. Si l'action de G sur S est sans point fixe, chaque place v dans Σ est décomposée dans K, et donc est de degré pair sur $\mathbf{F}$. Le degré de Δ est pair. Celui de Δ_1 est donc pair. Le dernier énoncé de la proposition est donc établi.

La proposition ci-dessus, et sa démonstration, peuvent paraître étonnants. On va montrer que ce résultat arithmétique est la conséquence d'un résultat purement algébrique.

Soit k un corps de caractéristique différente de 3. Le système d'équations

$$a_1x_1^3 + a_2x_2^3 = t = a_3x_3^3 + a_4x_4^3$$

définit une variété affine de dimension 3, lisse en dehors du point dont toutes les coordonnées sont nulles. Soit V le complémentaire de ce point, et soit $p : V \to \mathbf{A}_k^1$ la flèche définie par t. Soit X une k-compactification lisse de V, équipée d'un k-morphisme $p : X \to \mathbf{P}_k^1$ étendant p. On peut choisir X telle que, pour tout point M de $\mathbf{P}_k^1 \setminus \{0, \infty\}$, la fibre X_M soit simplement le produit des deux cubiques projectives lisses $a_1x_1^3 + a_2x_2^3 = tz^3$ et $a_3x_3^3 + a_4x_4^3 = tw^3$, en particulier soit géométriquement connexe (et lisse). Au-dessus du point zéro, la fibre X_0 est un diviseur de X dont une union de composantes, soit Δ, est la fermeture de la surface d'équation affine

$$a_1x_1^3 + a_2x_2^3 = 0 = a_3x_3^3 + a_4x_4^3$$

(les x_i n'étant pas tous nuls).

Proposition 3.5 *Le groupe de Brauer vertical* $\mathrm{Br}_{\mathrm{vert}}(X) \subset \mathrm{Br}(X)$ *relativement à* p *est réduit à l'image de* $\mathrm{Br}(k)$.

(Note : en l'absence d'un modèle projectif et lisse X, on pourrait établir l'énoncé en remplaçant le groupe $\mathrm{Br}(X)$ par le groupe de Brauer non ramifié $\mathrm{Br}_{nr}(k(X)/k)$.)

Démonstration Supposons d'abord que k contient une racine cubique de 1, soit ζ, laquelle définit une identification $\mathbf{Z}/3 = \mu_3$. Les fibres du morphisme $p : X \to \mathbf{P}_k^1$ au-dessus de tout point de $\mathbf{P}^1_k \setminus \{0, \infty\}$ possèdent une composante géométriquement intègre (on peut en fait choisir X tel que ces fibres soient simplement le produit de deux cubiques lisses). Soit $A \in \mathrm{Br}(k(t))$, d'exposant premier à la caractéristique de k, et dont l'image réciproque par p^* est non ramifiée sur X. Ses résidus aux points génériques des composantes des fibres X_M sont triviaux. Pour $M \notin \{0, \infty\}$, ceci implique que le résidu de A en M est trivial.

Soit $K = k((a_1/a_2)^{1/3}, (a_3/a_4)^{1/3})$. C'est une extension galoisienne de k de groupe de Galois G un quotient de $\mathbf{Z}/3 \times \mathbf{Z}/3$. Les composantes géométriques de Δ sont définies sur K. En $t = 0$, le résidu de A, qui appartient à $H^1(k, \mathbf{Q}/\mathbf{Z})$ doit s'annuler dans $H^1(K, \mathbf{Q}/\mathbf{Z})$, donc appartenir au groupe $H^1(G, \mathbf{Q}/\mathbf{Z})$, groupe annulé par 3. Ainsi ce résidu appartient au noyau de $H^1(k, \mathbf{Z}/3) \to H^1(K, \mathbf{Z}/3)$, i.e. au noyau de $k^*/k^{*3} \to K^*/K^{*3}$. Ce noyau est le groupe engendré par les classes a_1/a_2 et a_3/a_4. Soit donc

$$(a_1/a_2)^i.(a_3/a_4)^j \in k^*/k^{*3} = H^1(k, \mathbf{Z}/3)$$

le résidu de A en $t = 0$. Le résidu en $t = 0$ de l'algèbre $(t, (a_1/a_2)^i.(a_3/a_4)^j)_\zeta$ est précisément $(a_1/a_2)^i.(a_3/a_4)^j \in k^*/k^{*3} = H^1(k, \mathbf{Z}/3)$. L'algèbre $(t, (a_1/a_2)^i.(a_3/a_4)^j)_\zeta$ n'a pas de résidu en dehors de $t = 0$ et $t = \infty$. Ainsi $A - (t, (a_1/a_2)^i.(a_3/a_4)^j)_\zeta \in \mathrm{Br}(k(t))$ a ses résidus triviaux en tout point de $\mathbf{P}^1$ sauf peut-être en l'infini. Un résultat classique (Faddeev, cf. [15], §1.2) montre alors que $A - (t, (a_1/a_2)^i.(a_3/a_4)^j)_\zeta$ appartient à $\mathrm{Br}(k) \subset \mathrm{Br}(k(t))$.

Je dis que l'image de $(t, (a_1/a_2))_\zeta$ dans $\mathrm{Br}(k(X))$ appartient à l'image de $\mathrm{Br}(k)$. En effet, dans le corps des fonctions de X, on a l'égalité $t = a_1 x_1^3 + a_2 x_2^3$. Donc

$$(t, (a_1/a_2))_\zeta = (a_1 x_1^3 + a_2 x_2^3, a_1/a_2)_\zeta = (a_2, a_1/a_2)_\zeta + ((a_1/a_2)x_1^3 + x_2^3, a_1/a_2)_\zeta$$

et le symbole $((a_1/a_2)x_1^3 + x_2^3, a_1/a_2)_\zeta$ est nul (tout symbole $(\alpha, 1-\alpha)_\zeta$ avec $\alpha \neq 0, 1$ est nul). Le même argument vaut pour $(t, (a_3/a_4))_\zeta$. Ainsi l'image de A dans $\mathrm{Br}(k(X))$ vient de $\mathrm{Br}(k)$.

Si k ne contient pas de racine primitive cubique de 1, on passe au corps $k(\zeta)$, extension quadratique de k. Un argument un tout petit peu astucieux de corestriction-restriction permet d'établir le résultat à partir de celui déjà établi.

Nous pouvons maintenant déduire de la proposition algébrique précédente la première partie de la proposition arithmétique qui la précède.

Soit Σ un ensemble de places v de k contenant toutes les places v telles que l'un de $v(a), v(b), v(c), v(d)$ ne soit pas divisible par 3. Soit pour chaque place dans Σ, un élément $\gamma_v \in k_v^*$ tel que le système

$$ax^3 + by^3 = \gamma_v = cz^3 + dt^3$$

admette une solution dans k_v. Il existe alors $\gamma \in k^*$ tel que, pour toute place v de k, le système

$$ax^3 + by^3 = \gamma = cz^3 + dt^3$$

admette une solution dans k_v.

Démonstration La fibration $X/\mathbf{P}^1_k$ a seulement deux fibres non lisses ($\lambda = 0$ et $\lambda = \infty$). La combinaison du théorème 0.2 (a) (Theorem 2.2.1 de [13]) et de la proposition 3.5 ci-dessus donne le résultat.

Remarque La variété X est k-birationnelle au produit de $\mathbf{P}^1_k$ par la surface cubique lisse V d'équation $ax^3 + by^3 = cz^3 + dt^3$. Pour a, b, c, d généraux, on a $\mathrm{Br}(V)/\mathrm{Br}(k) = \mathbf{Z}/3$. On a donc $\mathrm{Br}(X)/\mathrm{Br}(k) = \mathbf{Z}/3$. Il existe donc un élément non trivial dans $\mathrm{Br}(X)$, mais cet élément n'est pas "vertical" par rapport à la fibration p. Il ne semble pas y avoir ici d'analogue de la condition (Alg) (condition (D) de [14]). On observera que l'analyse du §4 de [14] est spécifique aux fibrations $p : X \to \mathbf{P}^1_k$ dont la fibre est une courbe.

Remarque Il est intéressant de noter que les mêmes arguments donnent :

Soient $p \geq 2$ un nombre premier et k un corps global de caractéristique différente de p. Soient $a, b, c, d \in k^*$. Si pour chaque place v il existe $\gamma_v \in k_v^*$ tel que l'équation

$$ax^p + by^p = \gamma_v = cz^p + dt^p$$

ait une solution dans k_v, alors il existe $\gamma \in k^*$ tel que l'équation

$$ax^p + by^p = \gamma = cz^p + dt^p$$

ait une solution dans chaque k_v.

Sous des hypothèses raisonnables sur les coefficients a, b, c, d, peut-on trouver γ tel que de plus la p-torsion du groupe de Tate-Shafarevich de la jacobienne de la courbe $ax^p + by^p = \gamma$ et celui de la courbe $cz^p + dt^p = \gamma$ soit trivial ? Ceci suffirait à assurer l'existence d'un zéro-cycle de degré un sur la surface $ax^p + by^p = cz^p + dt^p$.

Le paragraphe 4 de [39] (Lemme de Fisher), où l'hypothèse que k ne contient pas les racines de l'unité est cruciale, ne requiert ici aucune modification.

Au paragraphe 5 de [39], on trouve au lemme 7 une utilisation du théorème de densité de Tchebotarev. La seule modification à apporter dans notre contexte est qu'il convient de remplacer, dans l'énoncé de ce lemme, les "premiers de degré (absolu) un" de K par les points fermés de C' qui sont de degré un par rapport à C, i.e. sont au-dessus de places de k (= points fermés de C) inertes dans l'extension K/k. Les points fermés de C' qui sont de degré 2 par rapport à C ont une densité de Dirichlet nulle. Le théorème 7 de [30] assure ici aussi l'existence de places de K du type requis. On pourrait d'ailleurs, dans [39] comme dans la situation analogue ici, raisonner directement avec l'extension non abélienne $F = K((a_1/a_2)^{1/3}, (a_3/a_4)^{1/3}, \xi^{1/3})/k$, en appliquant le théorème 7 de [30] à la classe de conjugaison de $\mathrm{Gal}(F/k)$ formée des éléments non triviaux induisant l'identité sur $K((a_1/a_2)^{1/3}, (a_3/a_4)^{1/3})$.

Immédiatement après la démonstration du lemme 7 de [39] on trouve une autre version du théorème de Tchebotarev (sous la forme du théorème de Dirichlet). Ici il convient d'une part de remplacer les "premiers de degré (absolu) un" de K par les points fermés de C' qui sont de degré un par rapport à C, d'autre part de choisir un sous-groupe ouvert convenable du groupe des idèles de K comme il a été fait (pour k) dans la discussion du paragraphe 3 (proposition établie ci-dessus).

L'argument extrêmement élaboré qui suit l'énoncé de la Condition 5 vaut tout autant dans le cas fonctionnel. On y trouve une utilisation du théorème de Tchebotarev (Dirichlet) deux paragraphes avant l'énoncé du théorème 3. On peut ici utiliser la forme suivante du théorème de Tchebotarev, qui m'a été communiquée par Serre :

Théorème 3.6 *Soit K un corps global. On se donne un ensemble fini S de places, contenant les places archimédiennes s'il y en a. On se donne pour chaque $v \in S$ un sous-groupe ouvert U_v du groupe multiplicatif local K_v^* ; on suppose qu'il existe au moins une place $v \in S$ pour laquelle U_v est d'indice fini dans K_v^* (c'est automatique si v est une place archimédienne). Soit, pour tout v dans S, un élément x_v de K_v^*. Alors il existe un élément x de K^* et une place w non dans S tels que l'on ait:*

(i) $x/x_v \in U_v$ pour $v \in S$;

(ii) x est une unité en toute place non dans S distincte de w;

(iii) x est une uniformisante en w.

Lors de la démonstration du théorème 3, à la fin du paragraphe 5, Swinnerton-Dyer doit faire une extension quadratique $k = k_0(\sqrt{\alpha})$. Ceci nous amène ici à nous limiter au cas où q est impair.

En retranscrivant les toutes dernières lignes avant le paragraphe 6, on a ici besoin de montrer : soit $C/\mathbf{F}$ une courbe projective, lisse, géométriquement connexe, soient $\mathbf{F}'/\mathbf{F}$ une extension quadratique et $C' = C \times_{\mathbf{F}} \mathbf{F}'$. Alors le groupe $\mathrm{Pic}(C')$ est engendré par des points fermés de degré un au-dessus de C. Pour l'établir, notons d'abord que le théorème de Tchebotarev garantit l'existence de points fermés de C décomposés dans l'extension C'/C. Soit $P \in C$ un tel point, et $Q_1, Q_2 \in C'$ les points de C' au-dessus de P. Le groupe $\mathrm{Pic}(C' \setminus \{Q_1, Q_2\})$ est un quotient fini de $\mathrm{Pic}(C')$ qui correspond à un revêtement abélien connexe C''/C'. Le théorème de Tchebotarev assure alors que ce groupe est engendré par les éléments de Frobenius associés à un nombre fini de points fermés de C' de degré un sur C. La réunion de ces points fermés et de $\{Q_1, Q_2\}$ engendre $\mathrm{Pic}(C')$.

Nous avons maintenant vérifié que la démonstration de Swinnerton-Dyer s'étend au cas où le corps k est un corps de fonctions d'une variable sur un corps fini $\mathbf{F}$, de caractéristique différente de 2 et 3, ne contenant pas de racine cubique non triviale de 1. Comme indiqué dans l'introduction, elle s'étend de façon inconditionnelle : nous allons en effet rappeler comment les résultats de Tate [42] impliquent la finitude des groupes de Tate-Shafarevich qui nous intéressent ici.

Théorème 3.7 *Soit $K = \mathbf{F}(C)$ le corps des fonctions d'une courbe C sur un corps fini $\mathbf{F}$, de caractéristique impaire première à 3. Soit $a \in K^*$. Le sous-groupe de torsion 3-primaire du groupe de Tate-Shafarevich de la K-courbe elliptique $x^3 + y^3 + at^3 = 0$ est un groupe fini.*

Démonstration Soit E_K la courbe elliptique définie sur K par $x^3 + y^3 + at^3 = 0$. Soit $L = K(a^{1/3})$. C'est une extension finie de K, de degré 1 ou 3. Le noyau de l'application de restriction $Ш(E_K) \to Ш(E_K \times_K L)$ est un sous-groupe de la 3-torsion de $Ш(E_K)$, et ce dernier groupe est fini. En effet, si $U \subset C$ est un ouvert de Zariski non vide au-dessus duquel la courbe E admet pour modèle un U-schéma abélien $\mathcal{E}/U$, la 3-torsion de $Ш(E_K)$ est un sous-quotient $H^1_{\text{ét}}(U, {}_3\mathcal{E})$, et ce groupe est clairement fini.

Pour établir le théorème, quitte à changer les notations, on peut supposer que a est un cube dans le corps de fonctions $K = \mathbf{F}(C)$, et donc que la courbe E_K n'est autre que la courbe "constante" $x^3 + y^3 + t^3 = 0$, vue comme courbe sur K. La courbe E_K admet alors pour modèle au-dessus de C le produit $X = E \times_{\mathbf{F}} C$, où l'on note $E/\mathbf{F}$ la courbe d'équation $x^3 + y^3 + t^3 = 0$ sur $\mathbf{F}$.

Suivant (dans un cas très particulier) des arguments d'Artin et Tate ([41], Theorem 3.1; la démonstration est donnée au paragraphe 4 de l'article [16] de Grothendieck), on voit que $Ш(E_K)$ s'identifie au groupe de Brauer $\mathrm{Br}(X)$ de $X = E \times_{\mathbf{F}} C$.

Soit l premier différent de la caractéristique de $\mathbf{F}$, par exemple $l = 3$. Etant donnée une $\mathbf{F}$-variété projective et lisse W, la torsion l-primaire de $\mathrm{Br}(W)$ est finie si et seulement si la conjecture de Tate $T^1_l(W)$ vaut pour les diviseurs sur W ([41], Thm. 5.2, où l'énoncé est limité au cas des surfaces, qui nous suffirait ici; le résultat est général, voir [43], Prop. 4.3). Une des versions de cette conjecture dit que l'application naturelle

$$\mathrm{Pic}(W) \otimes_{\mathbf{Q}} \mathbf{Q}_l \to H^2_{\text{ét}}(W \times_{\mathbf{F}} \overline{\mathbf{F}}, \mathbf{Q}_l)(1))^{\mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})}$$

est un isomorphisme. La conjecture de Tate T^1_l pour une courbe est triviale. Si l'on connaît la conjecture T^1_l pour deux variétés W_1 et W_2, on la connaît pour leur produit. Cet énoncé difficile résulte, comme expliqué par Tate dans [40] et [42], de son théorème [42] selon lequel pour deux variétés abéliennes A et B sur un corps fini $\mathbf{F}$, la flèche

$$\mathbf{Q}_l \otimes \mathrm{Hom}_{\mathbf{F}}(A, B) \to \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})}(H^1(B), H^1(A))$$

est un isomorphisme. Ainsi la conjecture de Tate T_l^1 vaut pour $X = E \times_{\mathbf{F}} C$, produit de deux courbes (les deux variétés abéliennes A et B sont la courbe elliptique E d'une part, la jacobienne de C d'autre part.) Par l'équivalence mentionnée plus haut, on conclut que la torsion l-primaire de $\mathrm{Br}(X)$ est finie.

Remarque On peut en fait montrer que le groupe $\mathrm{Br}(X)$ tout entier est fini, voir [41], Thm. 5.2, pour la torsion première à la caractéristique, et les références (à un travail de Milne) après la proposition 4.3 de [43]. On peut ainsi voir que sous les hypothèses du théorème, la torsion première à la caractéristique de $\mathbf{F}$ du groupe de Tate-Shafarevich de la K-courbe elliptique

$$x^3 + y^3 + at^3 = 0$$

est un groupe fini. Ceci vaut plus généralement pour le groupe de Tate-Shafarevich de la jacobienne d'une $\mathbf{F}(C)$-courbe qui devient constante après extension finie de son corps de base.

Ceci achève d'établir le théorème 3.1 énoncé au début de ce chapitre. Le théorème 3.2 en résulte par une méthode de sections hyperplanes classique ([39], p. 911).

Bibliographie

[1] C. L. Basile et T. A. Fisher, Diagonal cubic equations in four variables with prime coefficients, *Rational points on algebraic varieties* (E. Peyre, Yu. Tschinkel, éd.), Progress in Mathematics, vol. 199 Birkhäuser, 2001, p. 1-12.

[2] A. O. Bender et Sir Peter Swinnerton-Dyer, Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in $\mathbf{P}^4$, Proc. London Math. Soc. (3) **83** (2001), 299-329.

[3] M. Borovoi et B. È. Kunyavskiĭ, Formulas for the unramified Brauer group of a principal homogeneous space of a linear algebraic group. J. Algebra **225** (2000), 804-821.

[4] J.-L. Colliot-Thélène, The Hasse principle in a pencil of algebraic varieties, *Number theory (Tiruchirapalli, 1996)*, Contemp. Math. vol. 210, Amer. Math. Soc., Providence, RI, 1998, p. 19-39.

[5] J.-L. Colliot-Thélène, Hasse principle for pencils of curves of genus one whose jacobians have a rational 2-division point, in *Rational points on algebraic varieties* (E. Peyre, Yu. Tschinkel, éd.), Progress in Mathematics, vol. Birkhäuser, 2001, p. 117-161.

[6] J.-L. Colliot-Thélène, D. Harari et A. N. Skorobogatov, Valeurs d'un polynôme à une variable représentées par une norme, prépublication (distribuée antérieurement sous le titre "Sur l'équation $P(t) = \mathrm{Norme}_{K/k}(\mathbf{z})$").

[7] J.-L. Colliot-Thélène et B. È. Kunyavskiĭ, Groupe de Brauer non ramifié des espaces principaux homogènes de groupes linéaires, J. Ramanujan Math. Soc. **13** (1998), 37-49.

[8] J.-L. Colliot-Thélène et B. Poonen, Algebraic families of nonzero elements of Shafarevich-Tate groups, J. Amer. Math. Soc. **13** (1) (1999), 83-99.

[9] J.-L. Colliot-Thélène et P. Salberger, Arithmetic on some singular cubic surfaces, Proc. London Math. Soc. (3) **58** (1989), 519-549.

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

[11] J.-L. Colliot-Thélène, J.-J. Sansuc et Sir Peter Swinnerton-Dyer, Intersections of two quadrics and Châtelet surfaces, I. J. reine angew. Math. **373** (1987) 37-107; II. J. reine angew. Math. **374** (1987), 72-168.

[12] J.-L. Colliot-Thélène et A. N. Skorobogatov, Descent on fibrations over $\mathbf{P}^1_k$ revisited, Math. Proc. Camb. Phil. Soc. **128** (2000), 383-393.

[13] J.-L. Colliot-Thélène, A. N. Skorobogatov et Sir Peter Swinnerton-Dyer, Rational points and zero-cycles on fibred varieties: Schinzel's hypothesis and Salberger's device. J. reine angew. Math. **495** (1998), 1-28.

[14] J.-L. Colliot-Thélène, A. N. Skorobogatov et Sir Peter Swinnerton-Dyer, Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, Invent. math. **134** (1998), 579-650.

[15] J.-L. Colliot-Thélène et Sir Peter Swinnerton-Dyer, Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties, J. reine angew. Math. **453** (1994), 49-112.

[16] A. Grothendieck, Le groupe de Brauer I, II, III. Exemples et compléments, *Dix exposés sur la cohomologie des schémas*, North-Holland, Amsterdam; Masson, Paris, 1968, p. 67-188.

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

[18] D. Harari, Flèches de spécialisations en cohomologie étale et applications arithmétiques, Bull. Soc. Math. France **125** (1997), 143-166.

[19] D. Harari, Weak approximation and fundamental groups, Ann. Sci. Éc. Norm. Sup. **33** (2000), 467-484.

[20] D. Harari, Groupes algébriques et points rationnels, Math. Ann. **322** (2002), 811-826.

[21] D. Harari et A. N. Skorobogatov, Non-abelian cohomology and rational points, Compositio Math. **130** (2002), 241-273.

[22] D. Harari et A. N. Skorobogatov, The Brauer group of torsors and its arithmetic applications, Max Planck Institut Preprint **33** (2002).

[23] D. R. Heath-Brown, The solubility of diagonal cubic diophantine equations, Proc. London Math. Soc. (3) **79** (1999), 241-259.

[24] D. R. Heath-Brown et A. N. Skorobogatov, On certain equations involving norms, Acta math. **189** (2002) 161-177.

[25] S. Lang, Sur les séries L d'une variété algébrique, Bull. Soc. Math. France **84** (1956), 385-407.

[26] Yu. I. Manin, Le groupe de Brauer-Grothendieck en géométrie diophantienne, *Actes du congrès intern. math. (Nice, 1970)*, Gauthier-Villars, Paris, 1971, vol. 1, p. 401-411 .

[27] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Boston, 1986.

[28] B. Poonen, The Hasse principle for complete intersections in projective space, in *Rational points on algebraic varieties* (E. Peyre, Yu. Tschinkel, éd.), Progress in Mathematics, vol. 199 Birkhäuser, 2001, p. 307-311.

[29] J-P. Serre, *Groupes algébriques et corps de classes*, Actualités scientifiques et industrielles **1264**, Hermann, Paris (1959).

[30] J-P. Serre, Zeta and L functions, *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, (O.F.G. Schilling, éd.), Harper and Row, New York, 1965, p. 82-92.

[31] J-P. Serre, *Cohomologie galoisienne*, Cinquième édition, révisée et complétée, LNM 5, Springer, 1994.

[32] A. N. Skorobogatov, Descent on fibrations over the projective line, Amer. J. of Math. **118** (1996), 905-923.

[33] A. N. Skorobogatov, Beyond the Manin obstruction, Invent. math. **135** (1999), 399-424.

[34] A. N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001.

[35] Sir Peter Swinnerton-Dyer, Rational points on certain intersections of two quadrics, *Abelian varieties* (W. Barth, K. Hulek and H. Lange, éd.), Walter de Gruyter, Berlin, 1995, p. 273-292.

[36] Sir Peter Swinnerton-Dyer, Rational points on some pencils of conics with 6 singular fibres. Ann. Fac. Sci. Toulouse Math. (6) **8** (1999), 331-341.

[37] Sir Peter Swinnerton-Dyer, Arithmetic on diagonal quartic surfaces, II, Proc. London Math. Soc. (3) **80** (2000), 513-544. Errata (à paraître).

[38] Sir Peter Swinnerton-Dyer, Weak approximation and R-equivalence on cubic surfaces, in *Rational points on algebraic varieties* (E. Peyre, Yu. Tschinkel, éd.), Progress in Mathematics, vol. 199, Birkhäuser, 2001, p. 359-406.

[39] Sir Peter Swinnerton-Dyer, The solubility of diagonal cubic surfaces, Ann. Sci. Éc. Norm. Sup. **34** (2001), 891-912.

[40] J. Tate, Algebraic cycles and poles of zeta functions, in *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)* (O.F.G. Schilling, éd.), Harper and Row, New York, 1965, p. 93-110.

[41] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Séminaire Bourbaki, Exp. 306, réimpression: *Séminaire Bourbaki, Années 1964/65-1965/66, Exposés 277-312.* Soc. Math. France, Paris, 1995.

[42] J. Tate, Endomorphisms of abelian varieties over finite fields. Invent. Math. **2** (1966), 134-144.

[43] J. Tate, Conjectures on algebraic cycles in l-adic cohomology, in *Motives* (U. Jannsen et al. éd.), Proc. Sympos. Pure Math., vol. 55.1, Amer. Math. Soc., Providence, RI, 1994, p. 71-83.

Jean-Louis Colliot-Thélène
CNRS, UMR 8628, Mathématiques,
Université de Paris-Sud,
Bâtiment 425,
F-91405 Orsay, France
Jean-Louis.Colliot-Thelene@math.u-psud.fr