Principe de Hasse et obstruction de Brauer-Manin

Cyril Demarche
sous la direction de David Harari

10 Octobre 2006

Table des matières

1 Généralités sur les variétés projectives

On s'intéresse à la recherche de points rationnels sur des variétés algébriques. Dans cet exposé, on considérera des variétés projectives sur un corps : si k est un corps parfait, on considère une cloture algébrique $\overline{k}$.

Définition 1. *Une variété algébrique projective sur k est définie comme étant un sous-ensemble de $\mathbf{P}^n(\overline{k})$ de la forme*

$$V(f_1,\dots,f_m) := \left\{(a_0:\dots:a_n)\in\mathbf{P}^n(\overline{k}) : f_i(a_0:\dots:a_n)=0 \text{ pour tout } i\right\}$$

où les f_i sont une famille finie de polynômes homogènes à coefficients dans k.

Une telle variété est naturellement munie d'une topologie, dite de Zariski, dont les fermés sont donnés par les variétés projectives incluses dans cette variété, à savoir les

$$V(I) := \left\{(a_0:\dots:a_n)\in\mathbf{P}^n(\overline{k}) : f(a_0:\dots:a_n)=0 \text{ pour tout } f\in I \text{ homogène }\right\}$$

où I est un idéal homogène de $k[X_0,\dots,X_n]$ contenant les f_i. Rappelons qu'un idéal homogène de $k[X_0,\dots,X_n]$ est un idéal engendré par des éléments homogènes.

Si cette variété est notée X, on notera $X(K)$ l'ensemble des solutions dans K^n du système $f_i(x)=0,\forall i$, pour toute extension K de k.

On dispose aussi de la notion de morphisme de k-variétés, qui consiste en une application entre variétés qui est polynomiale en les coordonnées. D'ailleurs, la donnée d'un K-point $P\in X(K)$ équivaut à celle d'un k-morphisme Spec $K \xrightarrow{P} X$

Une variété projective $V(f_1,\dots,f_m)$ sera dite lisse en un point $x\in X(\overline{k})$ si la matrice jacobienne $\left(\frac{\partial f_i}{\partial x_j}(x)\right)$ est de rang maximal.

Enfin, on dira qu'une variété projective X est irréductible si X n'est pas réunion de deux sous-variétés strictes.

Concrétement, si $k=\mathbf{Q}$, on dispose avec la notion de variété d'un cadre géométrique pour rechercher des solutions entières (ie dans $\mathbf{Z}^n$) du système polynomial $f_i(x)=0,\forall i$: une telle solution correspond à un point à coordonnées entières, dit point rationnel, de la variété étudiée, i.e. un point de $X(\mathbf{Q})$.

Un des objectifs de la géométrie arithmétique est donc de dégager des méthodes, des principes généraux qui permettent de déterminer si une variété (ou une famille de variété) donnée admet des points rationnels ou non.

2 Principe de Hasse et approximation faible

On remarque qu'un point rationnel de X à coordonnées dans $\mathbf{Z}$ donne naissance à une famille de solutions du système $f_i(\underline{x})=0,\forall i$ dans $\mathbf{Z}/p^r\mathbf{Z}$, pour tout nombre premier p et pour tout entier r. On s'intéresse en quelque sorte à une réciproque de cette construction.

Pour trouver des points rationnels, on s'intéresse aux complétés d'un corps de nombres : le théorème d'Ostrowski décrit les différentes valeurs absolues existant sur un corps de nombres k, à équivalence près (deux valeurs absolues sont équivalentes si elles définissent la même topologie sur k). Il s'agit des valeurs absolues $\mathfrak{P}$-adiques ($x\mapsto |x|_{\mathfrak{P}} := (N\mathfrak{P})^{-v_{\mathfrak{P}}(x)}$, où $\mathfrak{P}$ est un idéal premier de l'anneau des entiers de k de norme $N\mathfrak{P}$ et $v_{\mathfrak{P}}(x)$ l'exposant de $\mathfrak{P}$ dans la décomposition de l'idéal $x\mathcal{O}_k$ en idéaux premiers, et des valeurs absolues archimédiennes, de la forme $x\mapsto|\sigma(x)|$, $|.|$ désignant la valeur absolue usuelle sur $\mathbf{C}$ et σ étant l'un des $\mathbf{Q}$-plongements de k dans $\mathbf{C}$. De plus, ces valeurs absolues sont deux-à-deux non-équivalentes, et on appelle place du corps k une classe

d'équivalence de valeurs absolues sur k, on a donc une correspondance entre les places de k et les idéaux premiers de k, auxquels on ajoute les plongements complexes de k. Si on note v une place de k, on dispose d'une topologie induite par v sur k, pour laquelle on peut consédérer le complété k_v de k.

Par exemple, dans le cas du corps de nombres $\mathbf{Q}$, les places sont exactement les nombres premiers et la place infinie correspondant au plongement de $\mathbf{Q}$ dans $\mathbf{R}$ (i.e. la valeur absolue usuelle). Les complétés respectifs sont notés $\mathbf{Q}_p$, pour p premier, et $\mathbf{R}$ pour la place infinie. Le corps $\mathbf{Q}_p$ est appelé corps des nombres p-adiques. On a d'ailleurs une autre description de ce corps : si on note $\mathbf{Z}_p$ la limite projective des $\mathbf{Z}/p^n\mathbf{Z}$ pour les morphismes de réduction $\mathbf{Z}/p^{n+1}\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$, alors $\mathbf{Q}_p$ est isomorphe au corps des fractions de l'anneau $\mathbf{Z}_p$, $\mathbf{Z}_p$ étant appelé l'anneau des entiers de $\mathbf{Q}_p$. On peut décrire $\mathbf{Z}_p$ comme le sous-anneau du produit des $\mathbf{Z}/p^n\mathbf{Z}$ formé des familles (x_n), $x_n \in \mathbf{Z}/p^n\mathbf{Z}$, telles que la restriction de x_{n+1} modulo p^n soit x_n. On peut d'ailleurs voir les entiers p-adiques comme les sommes formelles $\sum_{n\in\mathbf{N}} a_n p^n$, avec $a_n \in \{0,\dots,n-1\}$, et les éléments de $\mathbf{Q}_p$ comme les sommes $\sum_{n\in\mathbf{Z}} a_n p^n$, avec $a_n \in \{0,\dots,n-1\}$ et $a_n = 0$ pour $n \leq n_0$, $n_0 \in \mathbf{Z}$. Pour plus de détails sur cette partie, on pourra consulter [13].

Disposant ainsi des différents complétés de k, la recherche de points rationnels est grandement facilitée lorsque la variété en question vérifie ce que l'on appelle le principe de Hasse :

Définition 2. *Soit k un corps de nombres. Soit $\mathcal{X}$ une famille de variétés projectives sur k. On dit que la famille $\mathcal{X}$ vérifie le principe de Hasse si pour toute variété X de $\mathcal{X}$, si pour toute place v de k, $X(k_v) \neq \emptyset$, alors $X(k) \neq \emptyset$.*

Dans ce cas, pour une variété X de la famille χ, il est relativement facile de décider si elle admet ou non des points rationnels, puisqu'il suffit de le tester localement en toutes les places de k, où l'on dispose d'outils du type lemme de Hensel par exemple (voir [13]) :

Lemme 1 (Hensel)**.** *Soient $f_1,\dots,f_n$ des polynômes en r-variables à coefficients dans $\mathbf{Z}_p$. On note $\overline{f_i}$ les réductions de ces polynômes modulo $p\mathbf{Z}_p$, que l'on voit comme des polynômes dans $\mathbf{Z}/p\mathbf{Z}$. Si le système $\overline{f_i}(\overline{x}) = 0, \forall i$ admet une solution lisse $\overline{x}_0 \in (\mathbf{Z}/p\mathbf{Z})^r$ (à savoir que la matrice jacobienne $\left(\frac{\partial \overline{f_i}}{\partial x_j}(\overline{x}_0)\right)$ est de rang maximal), alors cette solution se relève en une solution $x \in \mathbf{Z}_p^n$.*

Ce lemme permet par exemple de montrer très facilement qu'une conique de la forme $ax^2 + by^2 + c = 0$ admet des points locaux hors de la place 2 et des diviseurs des coefficients a, b et c.

Une autre question naturelle que l'on peut se poser lors de l'étude des points rationnels d'une variété est celle dite de l'approximation faible :

Définition 3. *On dit qu'une variété projective X sur un corps de nombres k vérifie l'approximation faible si l'ensemble des points rationnels $X(k)$ est dense dans l'espace topologique produit $\prod_v X(k_v)$, via l'injection diagonale ($X(k_v)$ est muni de la topologie induite par celle du corps topologique k_v). Si $\prod_v X(k_v)$ est non-vide, cela équivaut à la densité de $X(k)$ dans tous les $\prod_{v\in S} X(k_v)$, pour tout ensemble fini de places S.*

Quelques exemples :

Citons tout d'abord le fait que l'espace affine $\mathbf{A}_k^n$ satisfait l'approximation faible.

Concernant le principe de Hasse, l'exemple historique le plus célèbre est probablement le théorème de Hasse-Minkowski (voir par exemple [13]).

Théorème 2 (Hasse-Minkowski, 1924)**.** *Soit k un corps de nombres. Les quadriques projectives sur k vérifient le principe de Hasse. Cela signifie que pour une forme quadratique Q en n variables sur k, Q admet un zéro non-trivial dans k si et seulement si Q admet un zéro non trivial dans k_v pour toute place v de k.*

Le cas $n = 2$ est évident. Le cas $n = 3$ a été démontré par Legendre sur $\mathbf{Q}$ et par Hilbert sur un corps de nombres quelconque, le passage de $n = 3$ à $n = 4$, puis le cas $n \geq 5$, ont été montré par Minkowski dans la situation $k = \mathbf{Q}$, et Hasse a généralisé ces résultats dans le cas d'un corps de nombres quelconque.

Plus généralement, la théorie du corps de classes permet de démontrer le résultat suivant à propos de certaines équations normiques (voir [?]). Rappelons d'abord la définition suivante :

Définition 4. *Si K/k est une extension finie de corps, on définit la norme d'un élément x de K comme étant le déterminant de l'endomorphisme du k-espace vectoriel K $y \mapsto x.y$. On la note $N_{K/k}(x) \in k$. Une base $(e_i)_{1 \leq i \leq n}$ de K sur k étant fixée, l'équation $N_{K/k}(\sum_i x_i.e_i) = a$, avec $a \in k$, définit bien une équation polynomiale à coefficients dans k.*

Théorème 3 (Hasse, 1924)**.** *Soit E/F une extension cyclique de corps de nombres (i.e. une extension galoisienne de groupe de Galois cyclique). Un élément $a \in F$ est une norme dans l'extension E/F si et seulement si a est une norme dans toutes les extensions locales E_w/F_v, pour w divisant v, v parcourant les places de E.*

Cependant, on connait depuis longtemps des contrexemples au principe de Hasse. On peut citer par exemple la cubique sur $\mathbf{Q}$ d'équation $3x^3 + 4y^3 + 5z^3 = 0$ pour laquelle Selmer a montré en 1951 (voir [11]) qu'elle avait des points dans tous les $\mathbf{Q}_p$ et dans $\mathbf{R}$, mais pas dans $\mathbf{Q}$.

Un autre exemple est donné par une équation normique pour une extension abélienne non-cyclique : Hasse a montré que -1 est une norme locale partout dans l'extension $\mathbf{Q}(\sqrt{13}, \sqrt{17})/\mathbf{Q}$, mais que ce n'était pas une norme globale.

On cherche donc à expliquer ces contrexemples. On a besoin d'une obstruction plus fine que la vacuité d'un des $X(k_v)$ pour expliquer la vacuité de $X(k)$. On dispose ainsi par exemple de l'obstruction de Manin (ou de Brauer-Manin).

3 Obstruction de Brauer-Manin

Soit X une variété projective sur un corps de nombres k. On notera Ω l'ensemble des places de k. On note $\mathbf{A}_k$ l'anneau des adèles de k, à savoir le produit restreint des k_v par rapport aux anneaux d'entiers $\mathcal{O}_v$: cela signifie que c'est le sous-anneau du produit direct des k_v formé des éléments qui sont dans $\mathcal{O}_v$ pour presque toute place v.

On a besoin, pour définir cette obstruction, de la notion de groupe de Brauer d'un corps et d'une variété.

3.1 Groupe de Brauer

Pour plus d'informations sur le groupe de Brauer d'un corps, on peut par exemple regarder [12].

Définition 5. *Soit K un corps. Une K-algèbre simple centrale A est une K-algèbre simple dont le centre est K. Cela équivaut au fait que l'algèbre A soit isomorphe à une algèbre de matrices sur une algèbre à division (corps non-commutatif) de centre K. On dit que deux telles algèbres simples centrales sont équivalentes si les algèbres à division associées sont isomorphes.*

Définition 6. *L'ensemble des classes d'équivalence d'algèbres simples centrales sur un corps K (pour la relation d'équivalence définie au-dessus), muni du produit tensoriel, a une structure de groupe abélien, que l'on nomme groupe de Brauer de K, noté $Br\ K$.*

Pour généraliser cette définition, on a besoin de quelques notions de cohomologie galoisienne :

Définition 7. *Soit G un groupe profini, A un groupe abélien. On dit que A est un G-module discret si G agit sur A de façon continue (i.e. le stabilisateur de tout point de A est un sous-groupe ouvert de G), à savoir que pour cette action de G sur A, on a $A = \bigcup_U A^U$, U décrivant les sous-groupes ouverts de G.*

Définition 8. *Si on note $C^n(G, A)$ l'ensemble des applications continues de G^n dans A, on définit un morphisme $d_n : C^n(G, A) \to C^{n+1}(G, A)$ par*

$$d_n(f) : (g_1, \ldots, g_{n+1}) \mapsto g_1 f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n)$$

On obtient alors un complexe, dont la cohomologie est notée $H^n(G, A)$, à savoir $H^n(G, A) := Z^n(G, A)/B^n(G, A)$, où $Z^n(G, A)$ est l'ensemble des n-cocycles, à savoir $Ker(d_n)$, et $B^n(G, A)$ est l'ensemble des n-cobords, à savoir $Im(d_{n-1})$.

Citons la propriété de fonctorialité suivante, qui nous servira dans la suite.

Proposition 4. *Si on a un morphisme $f : G \to G'$ de groupes profinis, et A' un G'-module discret, alors f munit A' d'une structure de G-module discret, et on a un morphisme canonique $H^n(G', A') \xrightarrow{f^*} H^n(G, A')$.*

Muni de cet outil, on peut généraliser la définition du groupe de Brauer, en constatant que Br K coïncide avec le second groupe de cohomologie galoisienne $H^2(\Gamma_K, \overline{K})$ (Γ_K étant le groupe de Galois absolu du corps K), pour parler du groupe de Brauer-Grothendieck d'une K-variété algébrique :

Définition 9. *Soit X une K-variété (projective). On appelle groupe de Brauer (cohomologique) de X, et on note Br X, le groupe de cohomologie étale $H^2_{ét}(X, \mathbf{G}_m)$.*

Remarquons que sous certaines hypothèses (notamment la lissité de X), il existe une définition équivalente du groupe de Brauer de X faisant intervenir la notion d'algèbre d'Azumaya, qui est une généralisation immédiate de la notion d'algèbre simple centrale sur un corps. Mais l'équivalence de ces deux définitions est un résultat très difficile, et ici on s'intéressera seulement à la définition cohomologique.

Énonçons quelques propriétés importantes de ce groupe Br X.

Proposition 5. *Soit X une K-variété projective.*

- *$Br(Spec\ K) \cong Br\ K$.*
- *Si X est lisse, Br X se plonge dans le groupe Br $K(X)$.*
- *Le foncteur $Br(.)$ est un foncteur contravariant de la catégorie des k-variétés dans la catégorie des groupes abéliens.*
- *On dispose donc de morphismes canoniques Br $K \to$ Br X, dont on note $Br_0(X)$ l'image, et Br $X \to$ Br $\overline{X}$, dont on note $Br_1(X)$ le noyau.*
- *Si K est un corps local p-adique (extension finie de $\mathbf{Q}_p$), on a un isomorphisme :*

$$inv : Br\ K \cong \mathbf{Q}/\mathbf{Z}$$

- *Br* $\mathbf{R} \cong \mathbf{Z}/2\mathbf{Z}$
- *Br* $\mathbf{C} \cong 0$

Dans le cas des corps de nombres, le groupe de Brauer du corps s'intègre dans une suite exacte faisant intervenir les groupes de Brauer de tous les localisés de ce corps :

Théorème 6. *Si k est un corps de nombres, la théorie globale du corps de classes assure l'existence d'une suite exacte de groupes :*

$$1 \to Br\ k \to \bigoplus_v Br\ k_v \xrightarrow{\sum_v inv_v} \mathbf{Q}/\mathbf{Z} \to 1$$

où les $inv_v : Br\ k_v \to \mathbf{Q}/\mathbf{Z}$ proviennent des isomorphismes de la proposition précédente.

3.2 Obstruction de Brauer-Manin

Disposant de la notion de groupe de Brauer, on peut désormais définir l'obstruction de Brauer-Manin.

Pour toute ensemble fini S de places contenant les places infinies de k, on note $\mathcal{O}_{k,S}$ l'ensemble des éléments de k qui sont entiers hors de S, i.e. les $x \in k$ tels que $v(x) \geq 0$ pour tout $v \notin S$.

On a besoin du lemme technique suivant :

Proposition 7. *Si X est une k-variété projective, il existe un ensemble fini de places de k, noté S, et un $\mathcal{O}_{k,S}$-schéma propre $\mathcal{X}$ tel que $X \cong \mathcal{X} \times_{\mathcal{O}_{k,S}} k$.*

On définit alors :

$$X(\mathbf{A}_k) = \prod_v{}' (X(k_v) : \mathcal{X}(\mathcal{O}_v))$$

où $\prod'$ désigne le produit restreint.

Concrétement, cela signifie que $\mathcal{X}$ est défini par des équations à coefficients dans $\mathcal{O}_{k,S}$, et que pour tout diagramme commutatif de la forme

$$\begin{array}{ccc} \text{Spec } k' & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow \\ \text{Spec } A & \longrightarrow & \text{Spec } \mathcal{O}_{k,S} \end{array}$$

où A est un anneau de valuation discrète et k' son corps des fractions, il existe un unique morphisme Spec $A \to \mathcal{X}$ faisant commuter :

$$\begin{array}{ccc} \text{Spec } k' & \longrightarrow & \mathcal{X} \\ \downarrow & \nearrow & \downarrow \\ \text{Spec } A & \longrightarrow & \text{Spec } \mathcal{O}_{k,S} \end{array}$$

C'est ce que l'on appelle le critère valuatif de propreté.

Ici, dans le cas où X est projective, on va construire un accouplement :

$$(.,.)_{\mathrm{BM}} : \mathrm{Br}(X) \times X(\mathbf{A}_k) \to \mathbf{Q}/\mathbf{Z}$$

qui va nous fournir une nouvelle obstruction au principe de Hasse.

Pour cela, étant donné k' corps quelconque, et K/k' une extension, on définit :

$$\begin{array}{ccc} \mathrm{Br}(X) \times X(K) & \longrightarrow & \mathrm{Br}(K) \\ (A, P) & \longmapsto & A(P) \end{array}$$

où pour tout point K-rationnel de X, $P : \mathrm{Spec}K \to X$, on a, par fonctorialité, une flèche

$$\begin{array}{ccc} \mathrm{Br}(X) & \longrightarrow & \mathrm{Br}(K) \\ A & \longmapsto & A(P) \end{array}$$

Pour le corps de nombres k, la théorie locale du corps de classe fournit des invariants locaux pour tout $v \in \Omega$: $\mathrm{inv}_v : \mathrm{Br}(k_v) \hookrightarrow \mathbf{Q}/\mathbf{Z}$ (qui sont des isomorphismes aux places non-archimédiennes). On utilise alors la proposition précédente 7 : on dispose d'un modèle $\mathcal{X}$ propre sur $\mathcal{O}_{k,S}$. On remarque que si $v \notin S$, et $P_v : \mathrm{Spec}\ k_v \to X_v$ est un point k_v-rationnel de X_v, alors le critère valuatif de propreté (par propreté de la flèche verticale de droite) assure l'existence d'un diagramme commutatif :

$$\begin{array}{ccc} \mathrm{Spec}\ k_v & \xrightarrow{P_v} & \mathcal{X}_v \\ \downarrow & \nearrow & \downarrow \\ \mathrm{Spec}\ \mathcal{O}_v & \xrightarrow{=} & \mathrm{Spec}\ \mathcal{O}_v \end{array}$$

D'où $X_v(k_v) = \mathcal{X}_v(\mathcal{O}_v)$, c'est à dire que le k_v-point P_v est en fait un point de $\mathcal{X}$ à coordonnées dans l'anneau local $\mathcal{O}_v$, d'où finalement :

Proposition 8. *Si X est une variété projective sur k, alors*

$$X(\mathbf{A}_k) = \prod_v{}' (X(k_v) : \mathcal{X}(\mathcal{O}_v)) = \prod_v X(k_v)$$

On se donne alors $(P_v) \in X(\mathbf{A}_k)$, et $A \in \mathrm{Br}X$. Quitte à augmenter S, on peut supposer que $P_v \in \mathcal{X}(O_v)$ pour toute place v hors de S, et puisque $\mathrm{Br}\ X = \varinjlim_U \mathrm{Br}\ \mathcal{X}_U$, U décrivant les ouverts non-vides de $\mathrm{Spec}(\mathcal{O}_{k,S})$ (voir [6], lemme 1.16.) , il existe un ouvert non-vide U de $\mathrm{Spec}(\mathcal{O}_{k,S})$ tel que A est dans l'image du morphisme $\mathrm{Br}\ \mathcal{X}_U \to \mathrm{Br}\ X$. Donc, quitte à augmenter encore S (et remplacer $\mathcal{X}$ par $\mathcal{X}_U$), on peut supposer que $P_v \in \mathcal{X}(O_v)$, et $A \in \mathrm{Br}\ \mathcal{X}$ pour toute place v hors de S. Dans ce cas, $A(P_v) \in \mathrm{Br}(O_v) := \mathrm{Br}(\mathrm{Spec}\ O_v)$. Or on sait que $\mathrm{Br}(O_v) = 0$ (voir par exemple [6]), donc $\mathrm{inv}_v(A(P_v)) = 0$ pour v hors de S.

On peut alors définir l'accouplement de Brauer-Manin :

$$\begin{array}{ccc} \mathrm{Br}(X) \times X(\mathbf{A}_k) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ (A, (P_v)_{v\in\Omega}) & \longmapsto & \sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) \end{array}$$

qui est bien défini car la somme en question est finie.

On notera alors $X(\mathbf{A}_k)^{\mathrm{Br}}$ l'ensemble des éléments de $X(\mathbf{A}_k)$ orthogonaux à $\mathrm{Br}(X)$ sous cet accouplement. Or la loi de réciprocité globale, provenant de la théorie du corps de classe, assure que la suite suivante est exacte :

$$0 \to \mathrm{Br}(k) \to \bigoplus_{v\in\Omega} \mathrm{Br}(k_v) \xrightarrow{\sum} \mathbf{Q}/\mathbf{Z} \to 0$$

où $\sum$ est la somme des invariants locaux. Donc, si A est un élément de $\mathrm{Br}(X)$, et $P \in X(k)$, la famille $(A(P_v))_{v\in\Omega}$ de $\bigoplus_{v\in\Omega} \mathrm{Br}(k_v)$ provient de l'élément $A(P) \in \mathrm{Br}(k)$, et donc par exactitude de la suite (par le fait que c'est un complexe en fait), $\sum_{v\in\Omega} \mathrm{inv}_v(A(P_v)) = 0$. Par conséquent, le plongement diagonal $X(k) \hookrightarrow X(\mathbf{A}_k)$ se factorise au travers de $X(\mathbf{A}_k)^{\mathrm{Br}}$. Et on a même une injection de l'adhérence de $X(k)$ (dans $X(\mathbf{A}_k)$) dans le sous-ensemble $X(\mathbf{A}_k)^{\mathrm{Br}}$. Par conséquent, l'existence d'un point rationnel sur la variété X implique la non vacuité de $X(\mathbf{A}_k)^{\mathrm{Br}}$. On peut donc bien définir ainsi une obstruction à l'existence de point rationnel :

Définition 10 (Manin, 1970)**.** *Avec les notations précédentes, on dira que X est un contrexemple au principe de Hasse si $X(k) = \emptyset$ alors que $X(\mathbf{A}_k) \neq \emptyset$. On dit qu'un tel contrexemple est expliqué par l'obstruction de Brauer-Manin si $X(\mathbf{A}_k)^{Br}$ est vide. On dit que cette obstruction est la seule pour une variété X lorsque $X(\mathbf{A}_k)^{Br} \neq \emptyset$ implique que $X(k) \neq \emptyset$. De même pour l'approximation faible, on dit qu'un contrexemple X à l'approximation faible est expliqué par cette obstruction si $\overline{X(k)} \neq X(\mathbf{A}_k)^{Br}$, et que cette obstruction est la seule si $\overline{X(k)} = X(\mathbf{A}_k)^{Br}$.*

Manin a défini cette obstruction en 1970. Et il a fallu attendre Skorobogatov en 1999 pour construire un exemple de variété pour laquelle l'obstruction de Brauer-Manin n'est pas la seule, à savoir une variété X telle que $X(k) = \emptyset$ alors que $X(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$ (voir [15]). Ce contrexemple est une surface dite bi-elliptique, à savoir le quotient du produit de deux courbes elliptiques par un groupe finit agissant sans point fixe.

On connaît plusieurs familles de variétés qui ne vérifient pas le principe de Hasse, mais pour lesquelles l'obstruction de Brauer-Manin est la seule, à savoir des variétés X pour lesquelles $X(\mathbf{A}_k)^{\mathrm{Br}} \neq \emptyset$ implique que $X(k) \neq \emptyset$.

Citons quelques exemples :

D'abord, Colliot-Thélène, Sansuc et Swinnerton-Dyer ont montré en 1987 que pour les surfaces de Chatelet de la forme :

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

avec $a \neq 0$ et P polynôme de degré 4, les obstructions de Brauer-Manin au principe de Hasse et à l'approximation faible sont les seules.

Avant de parler d'une autre famille d'exemples pour lesquels l'obstruction de Brauer-Manin est la seule, on a besoin de quelques généralités sur les variétés abéliennes.

3.3 Variétés abéliennes, groupe de Tate-Shafarevich

Définition 11. *Une variété abélienne sur le corps k est une k-variété projective lisse connexe A munie de morphismes de variétés $m : A \times A \to A$ et $i : A \to A$, et d'un point rationnel $\epsilon \in A(k)$ munissant l'ensemble $A(\overline{k})$ d'une structure de groupe (nécessairement abélien) pour la multiplication m, l'inverse i et le neutre ϵ.*

Par exemple, une courbe elliptique est une variété abélienne de dimension 1.

Sur les variétés abéliennes, on dispose du théorème suivant :

Théorème 9 (Mordell-Weil, 1928)**.** *Soit k un corps de nombres, et A une variété abélienne sur k. Alors le groupe $A(k)$ des points rationnels de A est un groupe abélien de type fini.*

Ce théorème a été démontré par Mordell en 1922 pour les courbes elliptiques sur $\mathbf{Q}$ et généralisé par Weil en 1928.

Il existe une notion de variété abélienne : étant donnée une variété abélienne A, on notera A^* sa variété abélienne duale. Cette variété duale est caractérisée par le fait que $A^*(k)$ est canoniquement isomorphe au groupe abélien $\mathrm{Ext}_k(A, \mathbf{G}_m)$. On rappelle que pour deux groupes algébriques sur k notés G' et G'', le groupe $\mathrm{Ext}_k(G'', G')$ est défini comme les classes d'extensions (suites exactes courtes de k-groupes algébriques)

$$0 \to G' \to G \to G'' \to 0$$

où l'on identifie les extensions G et $\widetilde{G}$ lorsqu'il existe un morphisme $G \to \widetilde{G}$ (nécessairement un isomorphisme) faisant commuter le diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle =} & & \downarrow & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & G' & \longrightarrow & \widetilde{G} & \longrightarrow & G'' & \longrightarrow & 0 \end{array}$$

La structure de groupe abélien s'obtient de la façon suivante : si G et $\widetilde{G}$ sont deux extensions, alors on définit G_0 comme le produit fibré de G et $\widetilde{G}$ au-dessus de G'', et $\overline{G}$ comme le quotient de G_0 par l'image de G' par $g' \mapsto (g', -g')$. Alors on a une extension $0 \to G' \to \overline{G} \to G'' \to 0$, qui est la somme des deux extensions de départ. On vérifie que cela munit bien $\mathrm{Ext}_k(G'', G')$ d'une structure de groupe abélien.

Revenons aux variétés abéliennes sur k. On veut définir le groupe de Tate-Shafarevich d'une variété abélienne.

Définissons pour un Γ_k-module discret M, les groupes $Ш^i(k, M)$.

Définition 12. *Soit k un corps de nombres, M un Γ_k-module discret. On note $H^i(k, M) := H^i(\Gamma_k, M)$. On définit alors*

$$Ш^i(k, M) := Ker\left[H^i(k, M) \to \prod_v H^i(k_v, M)\right]$$

En remarquant que pour une k-variété X, Γ_k agit continûment sur l'ensemble $X(\overline{k})$,on peut désormais définir le groupe de Tate-Shafarevich d'une variété abélienne :

Définition 13. *Si k est un corps de nombres et A une k-variété abélienne, on définit son groupe de Tate-Shafarevich par $Ш(A) := Ш^1(k, A(\overline{k}))$.*

Le groupe $Ш(A)$ est très mystérieux, sa finitude dans le cas général n'étant pour l'heure qu'une conjecture, reliée à la fameuse conjecture de Birch et Swinnerton-Dyer.

On dispose du résultat de dualité suivant (voir par exemple [7]) :

Théorème 10 (Cassels-Tate)**.** *Soit A une variété abélienne sur un corps de nombres k. Alors il existe un accouplement bilinéaire*

$$Ш(A) \times Ш(A^*) \xrightarrow{<.,.>_{CT}} \mathbf{Q}/\mathbf{Z}$$

qui réalise une dualité parfaite entre les groupes :

$$Ш(A)/Ш(A)_{div} \times Ш(A^*)/Ш(A^*)_{div} \xrightarrow{<.,.>_{CT}} \mathbf{Q}/\mathbf{Z}$$

3.4 Torseurs sous une variété abélienne

On s'intéresse à l'obstruction de Brauer-Manin sur des variétés qui sont des k-torseurs sous une variété abélienne. Faisons d'abord quelques rappels sur la notion de torseur (voir [16]) :

Définition 14. *Soit A une variété abélienne sur k. Un k-torseur (à droite) sous A est une k-variété projective X munie d'une action (à droite) de A (i.e. un morphisme de variétés $X \times A \to X$) faisant de $X(\overline{k})$ un espace principal homogène sous le groupe $A(\overline{k})$ (i.e. $X(\overline{k})$ est muni d'une action libre et transitive du groupe $A(\overline{k})$). On dit qu'un tel torseur X est trivial s'il est isomorphe à G, muni de l'action de G sur lui-même par translation à droite. Cela équivaut à dire que la k-variété X possède un point rationnel, i.e. $X(k) \neq \emptyset$.*

On sait relier les classes d'isomorphisme de torseurs sous A et la cohomologie galoisienne de A :

Proposition 11. *On dispose d'un isomorphisme d'ensembles pointés :*

$$H^1(k, A) \cong \{\textit{classes d'isomorphisme de } k\textit{-torseurs sous } A\}$$

La définition de la variété abélienne duale assure l'existence d'un morphisme $\varphi : H^1(k, A^*) \to \mathrm{Br}\ X/\mathrm{Br}_0(X)$. On note $\rho : \mathrm{Br}\ X \to \mathrm{Br}\ X/\mathrm{Br}_0(X)$ la projection, et $B := \rho^{-1}(\varphi(Ш(A^*))) \subset \mathrm{Br}\ X$.

Le théorème suivant (voir [5]) va nous permettre de construire des exemples de variétés pour lesquelles l'obstruction de Brauer-Manin au principe de Hasse est la seule.

Théorème 12 (Manin, 1970)**.** *Soit toujours X un k-torseur sous A. Soit $a \in B$, $\rho(a) = \varphi(a')$, avec $a' \in Ш(A^*)$ par définition. On suppose $X(\mathbf{A}_k) \neq \emptyset$, et on prend $(x_v) \in X(\mathbf{A}_k)$ quelconque. On note $b \in Ш(A)$ la classe d'isomorphisme du torseur X (pour toute place v, X_v admet un point rationnel dans k_v par hypothèse, donc est un k_v-torseur trivial sous A_v, et donc il est nul dans $H^1(k_v, A)$). Alors*

$$(a, (x_v)_v)_{BM} =< b, a' >_{CT}$$

Ce théorème important relie donc l'accouplement de Brauer-Manin à celui de Cassels-Tate. Or on a un résultat de non-dégénérescence pour ce dernier, on peut donc en déduire des résultats quant à l'obstruction de Brauer-Manin :

Corollaire 13. *Avec les notations précédentes, si $X(\mathbf{A}_k)^B \neq \emptyset$, alors $b \in Ш(A)_{div}$.*

Démonstration : En effet, on prend $(x_v) \in X(\mathbf{A}_k)^B$, et alors $\sum_v \mathrm{inv}_v(a(x_v)) = 0$ pour tout $a \in B$, donc grâce au théorème 12 de Manin, $< b, a' >_{\mathrm{CT}} = 0$ pour tout $a' \in Ш(A^*)$, et donc par le théorème 10 de dualité globale de Cassels-Tate, $b \in Ш(A)_{\mathrm{div}}$. □

Corollaire 14. *Si le groupe de Tate-Shafarevich $Ш(A)$ est fini, alors l'obstruction de Brauer-Manin relative au sous-groupe B est la seule, i.e.*

$$X(\mathbf{A}_k)^B \neq \emptyset \Rightarrow X(k) \neq \emptyset$$

Démonstration : $Ш(A)$ est fini, donc $Ш(A)_{\mathrm{div}} = 0$, donc si $X(\mathbf{A}_k)^B \neq \emptyset$, $b = 0$ par le corollaire précédent, donc X est un k-torseur trivial sous A, donc il possède des points rationnels. □

Cela fournit donc une famille de variétés pour lesquelles on sait que l'obstruction de Brauer-Manin est la seule. Reste cependant à tester l'hypothèse de finitude du groupe de Tate-Shafarevich. Citons par exemple un résultat inconditionnel sur la finitude de tels groupes (voir [10]) :

Théorème 15 (Rubin, 1987)**.** *Soit E une courbe elliptique sur $\mathbf{Q}$, à multiplication complexe (i.e. possédant d'autres endomorphismes que la multiplication par les entiers relatifs). Si la fonction L de la courbe E ne s'annule pas en $s = 1$, alors le groupe $Ш(E)$ est fini.*

Ce théorème n'est que le cas particulier d'une conjecture très générale, qui énonce la finitude du groupe de Tate-Shafarevich pour toute variété abélienne sur un corps de nombres.

Citons pour finir le résultat (inconditionnel) de Skorobogatov (voir [15]), qui utilise ce théorème :

Théorème 16 (Skorobogatov, 1999)**.** *La surface bielliptique sur $\mathbf{Q}$ d'équations affines*

$$(x^2 + 1)y^2 = (x^2 + 2)z^2 = 3(t^4 - 54t^2 - 117t - 243)$$

est un contrexemple au principe de Hasse pour lequel l'obstruction de Brauer-Manin n'est pas la seule, i.e. $X(k) = \emptyset$ alors que $X(\mathbf{A}_k^{Br}) \neq \emptyset$.

Ce résultat indique que l'obstruction de Brauer-Manin n'est pas la fin de l'histoire, et Skorobogatov a défini notamment des versions raffinées de cette obstruction qui permettent d'expliquer ce contrexemple.

Références

[1] J.W.S. Cassels et A. Fröhlich. *Algebraic number theory.* Academic press, London and New-York, 1967.

[2] J. Neukirch et A. Schmidt et K. Wingberg. *Cohomology of number fields.* Grundlehren der Mathematischen Wissenschaften, 323, Springer-Verlag, Berlin, 2000.

[3] A. Grothendieck. *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas.* Inst. Hautes Études Sci. Publ. Math. No. 32, 1967.

[4] R. Hartshorne. *Algebraic geometry.* Springer-Verlag, 1977.

[5] Y. I. Manin. Le groupe de Brauer-Grothendieck en géométrie diophantienne. *Actes du congrès international des Mathématiques, Nice, 1970*, 1 :401–411, 1971.

[6] J.S. Milne. *Etale Cohomology.* Princeton University Press, 1980.

[7] J.S. Milne. *Arithmetic duality theorems.* Notes Internet, 2006.

[8] D. Mumford. *Abelian varieties.* Tata Inst. Fund. Res. Studies in Math., 1970.

[9] J. Neukirch. *Algebraic number theory.* Springer, 1999.

[10] K. Rubin. Tate-Shafarevic groups and L-functions of elliptic curves with complex multiplication. *Inventiones Mathematicae*, (89) :527–559, 1987.

[11] E. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, (85) :203–362, 1951.

[12] J. P. Serre. *Corps locaux.* Hermann, 1959.

[13] J. P. Serre. *Cours d'arithmétique.* P.U.F., 1988.

[14] J. P. Serre. *Cohomologie galoisienne.* Lectures Notes Math. 5, 1994.

[15] A. Skorobogatov. Beyond the Manin obstruction. *Inventiones Mathematicae*, (135) :399–424, 1999.

[16] A. Skorobogatov. *Torsors and rational points.* Cambridge University Press, 2001.