Introduction au domaine de recherche

Olivier Wittenberg

27 septembre 2002

Résumé

Le texte qui suit constitue une brève introduction à quelques questions de géométrie arithmétique, dont le thème commun est l'étude des points rationnels des variétés algébriques. On y parlera notamment du principe de Hasse, de variétés abéliennes, du groupe de Tate-Shafarévitch et de la conjecture de Tate sur les cycles algébriques.

1 Introduction

Nombre de questions que l'on se pose en arithmétique concernent l'étude des solutions à coordonnées entières ou rationnelles de systèmes d'équations polynomiales à coefficients entiers. Étant donné un tel système, l'ensemble de ses solutions rationnelles est-il vide, fini ? S'il est infini, peut-on le décrire entièrement de manière satisfaisante ? Les solutions rationnelles sont-elles denses parmi les solutions complexes ? Existe-t-il un algorithme capable de dire s'il existe une solution rationnelle ? La géométrie arithmétique a pour vocation d'apporter des lumières sur ces questions au moyen de l'étude de la géométrie de l'ensemble des solutions *complexes* (ou, plus généralement, à valeurs dans un corps algébriquement clos) des systèmes considérés.

Nous emploierons par la suite le langage des variétés algébriques. Voici quelques « définitions » intuitives plus ou moins précises. Si k est un corps parfait (par exemple $\mathbb{Q}$), $\overline{k}$ une extension algébriquement close de k (par exemple $\mathbb{C}$), une *variété algébrique projective* sur k est une partie de $\mathbb{P}^n(\overline{k})$ de la forme

$$\left\{[x_0 : \ldots : x_n] \in \mathbb{P}^n(\overline{k})\,;\, \forall i \in \{1, \ldots, m\},\ f_i(x_0, \ldots, x_n) = 0\right\}$$

pour des polynômes homogènes f_i dans $k[X_0, \ldots, X_n]$ et un $n \in \mathbb{N}$. Une *variété algébrique affine* sur k est une partie de $\mathbb{A}^n(\overline{k}) = \overline{k}^n$ de la forme

$$\left\{x_1, \ldots, x_n \in \mathbb{A}^n(\overline{k})\,;\, \forall i \in \{1, \ldots, m\},\ f_i(x_1, \ldots, x_n) = 0\right\}$$

pour des polynômes f_i dans $k[X_1, \ldots, X_n]$ et un $n \in \mathbb{N}$. Dorénavant, le terme *variété projective* désignera toujours une variété algébrique projective géométriquement irréductible, i.e. qui n'est pas réunion de deux variétés algébriques projectives sur $\overline{k}$ distinctes de V. On dispose des notions de dimension d'une variété (on parle ainsi de *courbes* et de *surfaces* respectivement en dimensions 1 et 2), de morphisme entre variétés (ce sont les applications qui s'expriment à l'aide de polynômes en les coordonnées), de fonction rationnelle sur une variété (ce sont l'analogue des fonctions méromorphes en analyse complexe), de variété *lisse* (en tout point, l'espace tangent a la même dimension que la variété). La topologie de Zariski sur une variété projective (resp. affine) V est celle engendrée par la condition que les parties de $\mathbb{P}^n(\overline{k})$ (resp. $\mathbb{A}^n(\overline{k})$) incluses dans V et qui sont des variétés projectives (resp. affines) sont fermées dans V. En réalité, on considère les variétés de manière abstraite, c'est-à-dire indépendamment d'un plongement dans $\mathbb{P}^n(\overline{k})$ ou $\mathbb{A}^n(\overline{k})$, mais cela importe peu pour la suite. Si K est un sous-corps de $\overline{k}$ contenant k, on note $V(K)$ l'ensemble des points de V qui se trouvent dans $\mathbb{P}^n(K)$. On les appelle les *points K-rationnels* de V, ou simplement *points rationnels* si $K = k$.

Notons $(f_i)_{1 \leqslant i \leqslant m}$ une famille de polynômes homogènes de $\mathbb{Z}[X_0, \ldots, X_n]$. Remarquons qu'il revient au même d'étudier les points rationnels de la variété projective V sur $\mathbb{Q}$ définie par les f_i ou les solutions dans $\mathbb{Z}^m$ du système d'équations

$$\left\{\begin{array}{rcl} f_1(x_0, \ldots, x_n) & = & 0 \\ \vdots & & \\ f_m(x_0, \ldots, x_n) & = & 0, \end{array}\right. \tag{1}$$

puisque les f_i sont homogènes. Une solution dans $\mathbb{Z}^m$ de ce système en fournit une dans $(\mathbb{Z}/r\mathbb{Z})^m$ pour tout entier r, par réduction modulo r ; notamment, s'il n'existe pas de solution modulo r, il n'en existe aucune dans $\mathbb{Z}^m$. Cette remarque incite à considérer les équations modulo p^n, où p est un nombre premier. Pour $n = 1$, on est ainsi conduit à l'étude des points rationnels d'une variété[1] sur $\mathbb{F}_p$, le corps fini à p éléments. Notons $\mathbb{Z}_p$ l'ensemble des entiers p-adiques ; rappelons qu'il s'agit du complété (p)-adique de l'anneau $\mathbb{Z}$, c'est-à-dire la limite projective des $\mathbb{Z}/p^n\mathbb{Z}$ pour $n \in \mathbb{N}$, le morphisme de transition $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ étant la réduction modulo p^n. Son corps des fractions $\mathbb{Q}_p$ est le corps des nombres p-adiques, qui est aussi le complété de $\mathbb{Q}$ pour la valeur absolue p-adique. Étudier le système (1) modulo p^n pour tout $n \in \mathbb{N}$ revient à étudier ses solutions dans $\mathbb{Z}_p^m$, ce qui à son tour revient à étudier les points $\mathbb{Q}_p$-rationnels de V.

On voit bien à présent que l'on ne saurait se contenter de parler de variétés sur $\mathbb{Q}$, même si notre but est d'obtenir des résultats sur les points $\mathbb{Q}$-rationnels. Voici la liste des types de corps arithmétiquement intéressants que l'on a rencontrés :

1. les corps de nombres (i.e. les extensions finies de $\mathbb{Q}$), par exemple $\mathbb{Q}$;
2. les corps locaux (il s'agit de corps complets pour une valuation discrète), par exemple $\mathbb{Q}_p$;
3. les corps finis, par exemple $\mathbb{F}_p$.

On passe des corps de nombres aux corps locaux en les complétant par rapport à des valeurs absolues non-archimédiennes (i.e. correspondant à des distances ultramétriques), et l'on passe des corps locaux aux corps finis par considération du corps résiduel de l'anneau des entiers. Ajoutons à cette liste les corps de fonctions, i.e. les extensions de degré de transcendance 1 d'un corps fini. La pratique montre que de nombreux résultats sur les corps de nombres possèdent un analogue sur les corps de fonctions, souvent plus facile à démontrer. De même que l'on peut passer de $\mathbb{Q}$ à $\mathbb{F}_p$ en considérant l'anneau des entiers puis en réduisant modulo p, on peut passer d'un corps de fonctions K à un corps fini en considérant une courbe C projective et lisse dont les corps des fonctions rationnelles est isomorphe à K, puis en évaluant en un point x de C les fonctions rationnelles sur C qui y sont définies (dans le langage des schémas, il s'agit réellement de la même opération). C'est pourquoi on appelle *corps global* un corps qui est soit un corps de nombres, soit un corps de fonctions.

2 Topologie et arithmétique

Soit V une variété projective sur un corps de nombres K (on peut choisir $K = \mathbb{Q}$ pour fixer les idées). L'un des principes fondamentaux de la géométrie arithmétique est que la topologie de $V(\mathbb{C})$ doit influencer fortement le comportement arithmétique de V. Nous allons tenter de l'illustrer dans cette section, en prenant le cas des courbes algébriques projectives sur K.

Supposons donc que V soit une courbe projective et lisse. L'ensemble $V(\mathbb{C})$ est alors naturellement muni d'une structure de surface de Riemann compacte ; il est donc homéomorphe à un « tore à g trous », où g est le *genre* de V. Le genre est l'invariant le plus important associé à une courbe. Il peut se définir de manière purement algébrique (c'est par exemple la dimension sur K de l'espace des 1-formes différentielles régulières sur V, ou encore la dimension sur K du groupe de cohomologie $H^1(V, \mathscr{O}_V)$), mais on voit bien sur notre définition qu'il est de nature topologique.

2.1 Genre 0

Si $g = 0$, on montre facilement que V est isomorphe à une conique dans $\mathbb{P}^2$, à l'aide du théorème de Riemann-Roch (un plongement est donné par le faisceau anticanonique), d'où une équation homogène de la forme

$$ax^2 + by^2 + cz^2 = 0,$$

après un changement linéaire de coordonnées, avec $a, b, c \in K^\star$.

Proposition — *Soit $V(K) = \varnothing$, soit V est K-isomorphe à $\mathbb{P}^1$ et l'on peut expliciter tous les points rationnels de V une fois que l'on en a fixé un.*

[1] Remarquons que la variété sur $\mathbb{F}_p$ en question ne se déduit pas de V : il a fallu choisir un *modèle entier* de V, à savoir la donnée des f_i (par exemple, si l'on remplaçait f_1 par pf_1, on n'obtiendrait pas la même variété sur $\mathbb{F}_p$). Dans le langage des schémas, il s'agit d'un $\mathbb{Z}$-schéma dont la fibre générique est V. Dans certains cas, il existe un choix canonique.

Démonstration — Supposons qu'il existe un point rationnel $P \in V(K)$. Choisissons une droite D de $\mathbb{P}^2$, définie sur K mais ne passant pas par P. En tant que variété algébrique, elle est isomorphe à $\mathbb{P}^1$. Si T est un point de D, la droite passant par T et P coupe V en un unique autre point que P, puisque V est une conique ; appelons Q ce point (P et Q peuvent être confondus, si D est tangente à V). En associant Q à T, on vient de définir une application $D \to V$, qui est un morphisme bijectif de courbes projectives et lisses et donc un isomorphisme, ce qui montre que V est isomorphe à $\mathbb{P}^1$. De plus, on vérifie tout de suite que cet isomorphisme est défini sur K (si un polynôme du second degré à coefficients dans K possède une racine dans K, l'autre racine est aussi dans K).

Il est clair que l'on peut tout expliciter en écrivant une équation de D et en calculant les coordonnées de Q. Par exemple, dans le cas particulier $K = \mathbb{Q}$, $a = b = 1$, $c = -1$, on peut prendre $P = [0 : 1 : 1]$ et $D = \{[v : u : v] \in \mathbb{P}^2(\overline{k}) \,;\, [u : v] \in \mathbb{P}^1(\overline{k})\}$. Quelques calculs montrent alors que

$$Q = [2uv - 2v^2 : u^2 - 2uv : -u^2 + 2uv - 2v^2].$$

□

2.2 Genre 1

Supposons que $g = 1$ et que $V(K) \neq \varnothing$. Le couple formé par la donnée d'une courbe projective et lisse de genre 1 et d'un point rationnel de cette courbe est ce que l'on appelle une *courbe elliptique*. Le théorème de Riemann-Roch permet de prouver que toute courbe elliptique V est K-isomorphe à une cubique dans $\mathbb{P}^2$ d'équation

$$y^2 z = x^3 + axz^2 + bz^3,$$

où $a, b \in K$ sont tels que $4a^3 + 27b^2 \neq 0$, de sorte que le point rationnel distingué sur V soit $[0 : 1 : 0]$. Une telle équation s'appelle *équation de Weierstrass* ; réciproquement, si a et b sont des éléments de K tels que $4a^3 + 27b^2 \neq 0$, elle définit une courbe elliptique sur K.

L'ensemble des points rationnels de V peut être muni d'une structure de groupe abélien par la condition suivante : pour $P, Q, R \in V(K)$, on a $P + Q + R = 0$ si et seulement si P, Q et R sont alignés (dans $\mathbb{P}^2$). Le neutre est le point rationnel de coordonnées homogènes $[0 : 1 : 0]$; l'opposé du point $[x : y : z]$ est le point $[x : -y : z]$.

Théorème (Mordell-Weil) — *Le groupe $V(K)$ est de type fini.*

Il existe donc un entier $r \in \mathbb{N}$ et un groupe fini F tels que $V(K) \approx \mathbb{Z}^r \times F$. L'entier r est le *rang* de la courbe elliptique V. On conjecture qu'il existe des courbes elliptiques de rang arbitrairement grand sur $\mathbb{Q}$. Le théorème de Mordell-Weil répond en partie aux questions initiales sur les points rationnels de V : si $V(K)$ n'est pas vide, on peut le décrire entièrement dès que l'on en connaît un système de générateurs. On verra plus tard comment déterminer un tel système.

2.3 Genre $\geqslant 2$

Là encore, on dispose d'une réponse satisfaisante, mais sa démonstration est particulièrement difficile.

Théorème (Faltings, 1983) — *Si $g \geqslant 2$, $V(K)$ est fini.*

Les quelques résultats que l'on vient de décrire sur les points rationnels des courbes algébriques projectives justifient l'idée selon laquelle le genre d'une courbe gouverne son arithmétique. Par ailleurs, plus le genre est élevé, plus la situation est complexe à étudier. D'un point de vue qualitatif, cependant, le cas des courbes projectives et lisses est résolu ; en dimension supérieure, la détermination d'invariants géométriques[2] pertinents pour l'étude de l'arithmétique des variétés considérées est un thème de recherche important, sur lequel on sait encore très peu de choses à l'heure actuelle.

Comme autre exemple de l'existence de liens forts entre arithmétique et topologie des solutions complexes, mentionnons les conjectures de Weil, qui sont maintenant des théorèmes grâce à Dwork, Grothendieck et

[2] Un invariant est dit *géométrique* s'il peut se définir après extension des scalaires de K à $\mathbb{C}$.

Deligne. Soient k un corps fini de cardinal q, $\overline{k}$ une clôture algébrique de k, $\mathbb{F}_{q^r}$ l'unique sous-corps de $\overline{k}$ de cardinal q^r, V une variété projective et lisse sur k, de dimension n. On note N_r le cardinal de $V(\mathbb{F}_{q^r})$. Les entiers N_r sont d'un grand intérêt arithmétique ; pour les étudier, formons avec Weil la *fonction Zêta* de V : il s'agit de la série formelle

$$\zeta(V,t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right).$$

Une partie des conjectures de Weil affirme que $\zeta(V,t)$ est une fraction rationnelle de la forme $\zeta(V,t) = \prod_{i=0}^{2n} P_i(t)^{(-1)^{i+1}}$, où $P_i(t)$ est un polynôme à coefficients entiers, de coefficient constant 1, et dont les racines complexes sont les inverses d'entiers algébriques de module $q^{i/2}$. Notons que les P_i sont ainsi uniquement déterminés. On peut maintenant énoncer la partie des conjectures de Weil qui nous intéresse ici : s'il existe un sous-anneau A de $\mathbb{C}$, un idéal premier $\mathfrak{p}$ de A de corps résiduel k, des polynômes homogènes $(f_j)_{j\in J}$ à coefficients dans A dont les réductions modulo $\mathfrak{p}$ définissent la variété V, et si de plus les f_j vérifient une certaine condition de régularité (à savoir, la lissité du le A-schéma projectif qu'ils définissent), alors le degré de P_i est égal au i-ème nombre de Betti de l'espace topologique $X(\mathbb{C})$, en notant X la variété projective sur $\mathbb{C}$ définie par les f_j. (Rappelons que le i-ème nombre de Betti d'un espace topologique est la dimension de son i-ème groupe de cohomologie singulière.)

3 Principe de Hasse

Il est plus aisé d'étudier les points rationnels d'une variété sur un corps local que sur un corps global : un seul nombre premier entre en jeu, et la valuation du corps local induit une topologie sur l'ensemble des points rationnels. Par exemple, le théorème des fonctions implicites habituellement énoncé sur $\mathbb{R}$ et $\mathbb{C}$ vaut sur tout corps local, de sorte qu'une variété lisse sur un corps local possédant un point rationnel en possède « beaucoup », ce qui élimine les questions de densité des points rationnels.

Soit k un corps de nombres. On appelle *place* de k une classe d'équivalence de valeurs absolues non triviales sur k. Si v est une place de k, on note k_v le complété de k par rapport à v. Une place est *finie* si la valeur absolue correspondante est non-archimédienne, *infinie* sinon. Une place infinie est *réelle* ou *complexe* selon que le complété est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$. Par exemple, les places finies de $\mathbb{Q}$ sont en bijection avec les nombres premiers (p est associé à la valeur absolue p-adique) et $\mathbb{Q}$ possède une unique place infinie (la valeur absolue usuelle), qui est réelle ; les complétés de $\mathbb{Q}$ sont donc les $\mathbb{Q}_p$ et $\mathbb{R}$. Une variété possédant un point k-rationnel possède a fortiori un point k_v-rationnel pour toute place v. La question de la validité de la réciproque se pose naturellement.

Définition — *Soit $\mathscr{V}$ une classe de variétés algébriques sur k. On dit que $\mathscr{V}$* vérifie le principe de Hasse *(ou encore* le principe local-global*) si tout $X \in \mathscr{V}$ vérifiant $X(k_v) \neq \varnothing$ pour toute place v possède un point rationnel.*

3.1 Résultats positifs

On connaît de nombreuses classes de variétés vérifiant le principe de Hasse. Citons-en quelques-unes.

Théorème (Hasse, 1924) — *Une forme quadratique à coefficients dans un corps de nombres k possède un zéro non trivial dans k si et seulement si elle en possède un dans k_v pour toute place v de k. Autrement dit, les quadriques projectives vérifient le principe de Hasse.*

Ce théorème fut d'abord établi par Legendre lorsque $k = \mathbb{Q}$ pour des formes quadratiques en 3 variables. Il permet de prouver quelques énoncés élémentaires d'arithmétique, comme le théorème de Gauss selon lequel tout entier naturel est somme de trois nombres triangulaires. Un autre corollaire est que les courbes projectives et lisses de genre 0 sur k vérifient le principe de Hasse ; en effet, on a vu qu'une telle courbe est isomorphe à une conique dans $\mathbb{P}^2$. Voici maintenant un résultat de type local-global concernant les normes des extensions cycliques.

Théorème (Hasse, 1924) — *Soient K/k une extension cyclique de corps de nombres, $(\omega_1, \ldots, \omega_n)$ une base du k-espace vectoriel K, a un élément de k et V la variété affine sur k définie par l'équation*

$$a = N_{K/k}\left(\sum_{i=1}^{n} x_i\omega_i\right)$$

où $N_{K/k}$ désigne l'application norme de K à k. Alors V vérifie le principe de Hasse. Autrement dit, a est une norme dans l'extension K/k si et seulement s'il en est une partout localement.

Le principe de Hasse et la théorie du corps de classes sont intimement liés ; cette dernière est très souvent utilisée pour prouver la validité du principe de Hasse. Par exemple, le théorème précédent est une conséquence immédiate de la suite exacte fondamentale de la théorie du corps de classes global. Rappelons son énoncé.

Si K est un corps, on appelle *groupe de Brauer* de K et l'on note $\mathrm{Br}(K)$ le groupe de cohomologie galoisienne $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\star)$, où $\overline{K}$ est une clôture séparable de K. Il est fonctoriel en K, c'est-à-dire que si K est un sous-corps de L, on dispose d'un morphisme naturel $\mathrm{Br}(K) \to \mathrm{Br}(L)$. Notamment, le groupe de Brauer de K s'envoie dans celui de chacun de ses complétés. Si k est un corps de nombres et v une place de k, il y a une injection $\mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$, appelée *invariant en v* et notée inv_v. C'est un isomorphisme si v est finie. La théorie du corps de classes global affirme entre autres que la suite

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{2}$$

est exacte (ce qui sous-entend que la première flèche arrive bien dans la somme directe des $\mathrm{Br}(k_v)$). Si K est une extension finie galoisienne de k, le noyau de la flèche $\mathrm{Br}(k) \to \mathrm{Br}(K)$ s'identifie à $H^2(\mathrm{Gal}(K/k), K^\star)$ (théorème de Hilbert 90 et suite exacte d'inflation-restriction). Si de plus K/k est cyclique, on obtient ainsi canoniquement $k^\star/N_{K/k}K^\star = \mathrm{Ker}(\mathrm{Br}(k) \to \mathrm{Br}(K))$: le dernier théorème cité découle donc de l'injectivité de la flèche $\mathrm{Br}(k) \to \prod_v \mathrm{Br}(k_v)$ de la suite exacte (2).

Théorème (Châtelet, 1945) — *Le principe de Hasse vaut pour les variétés de Severi-Brauer sur k.*

Démonstration — Une variété de Severi-Brauer est une variété projective sur k qui est $\overline{k}$-isomorphe à un espace projectif $\mathbb{P}^m$; c'est ce que l'on appelle une *forme tordue* de $\mathbb{P}^m$. Par exemple, les courbes projectives et lisses de genre 0 en sont. En effet, elles possèdent un point $\overline{k}$-rationnel et sont donc $\overline{k}$-isomorphes à $\mathbb{P}^1$, d'après ce que l'on a vu. Les formes tordues d'un objet X sur k sont classifiées par le groupe de cohomologie non abélienne $H^1(G, \mathrm{Aut}_{\overline{k}}(X))$, où $\mathrm{Aut}_{\overline{k}}(X)$ désigne le groupe des $\overline{k}$-automorphismes de X et G le groupe de Galois de $\overline{k}$ sur k. Les automorphismes de $\mathbb{P}^m$ sont tous linéaires, c'est-à-dire que la suite évidente

$$1 \longrightarrow \overline{k}^\star \longrightarrow GL_{m+1}(\overline{k}) \longrightarrow \mathrm{Aut}_{\overline{k}}(\mathbb{P}^m) \longrightarrow 0$$

est exacte. En passant aux invariants sous G, on en déduit une application $H^1(G, \mathrm{Aut}_{\overline{k}}(\mathbb{P}^m)) \to \mathrm{Br}(k)$, dont le théorème de Hilbert 90 montre qu'elle est injective. Ainsi, à une variété de Severi-Brauer est associée une classe dans le groupe de Brauer de k. On peut montrer qu'une variété de Severi-Brauer est triviale (i.e. k-isomorphe à $\mathbb{P}^m$) si et seulement si elle possède un point rationnel. Le théorème de Châtelet est donc lui aussi une conséquence de la suite exacte (2). □

3.2 Variétés abéliennes et groupe de Tate-Shafarévitch

Les courbes projectives et lisses de genre 1, en revanche, ne vérifient pas toujours le principe de Hasse. Par exemple, la courbe projective d'équation

$$3x^3 + 4y^3 + 5z^3 = 0$$

est lisse et de genre 1 mais ne possède pas de point $\mathbb{Q}$-rationnel, tandis qu'elle possède des points dans chaque complété de $\mathbb{Q}$ (cet exemple est dû à Selmer). Nous allons définir ici un groupe mesurant l'obstruction au principe de Hasse pour ces courbes.

Avant tout, introduisons les variétés abéliennes. Ce sont, par définition, les variétés projectives lisses et connexes dont les points $\overline{k}$-rationnels sont munis d'une structure de groupe, automatiquement abélien. Les courbes elliptiques sont les variétés abéliennes de dimension 1. Les courbes algébriques et les variétés abéliennes sont les classes de variétés les plus « simples », d'une certaine manière ; ce sont d'abord sur elles que l'on teste les conjectures sur les variétés algébriques. À toute courbe projective et lisse C de genre g est associée une variété abélienne, que l'on appelle la *jacobienne* de C. Sa dimension est g. Si C possède un point rationnel, elle se plonge dans sa jacobienne ; ceci permet parfois de prouver des énoncés sur les courbe algébriques, sachant qu'ils sont vrais sur les variétés abéliennes. Signalons enfin que le théorème de Mordell-Weil énoncé plus haut pour les courbes elliptiques vaut plus généralement pour les variétés abéliennes : le groupe des points k-rationnels est de type fini.

Soit C une courbe projective et lisse de genre 1 sur k. Notons E sa jacobienne : c'est une courbe elliptique sur k. Il existe une action simplement transitive de E sur C, c'est-à-dire un morphisme $E \times C \to C$ induisant une action simplement transitive du groupe $E(\overline{k})$ sur $C(\overline{k})$ (on dit alors que C est un *torseur*, ou *espace principal homogène* sous E). Ainsi, afin d'étudier le principe de Hasse sur les courbes projectives et lisses de genre 1, il semble indiqué de considérer le principe de Hasse pour les torseurs sous les variétés abéliennes.

Soit A une variété abélienne sur k. Un torseur T sous A est dit *trivial* s'il est k-isomorphe à A, ce qui équivaut à l'existence d'un point rationnel de T. Les torseurs sous A sont classifiés par le groupe de cohomologie galoisienne $H^1(G, A(\overline{k}))$. On peut d'ailleurs expliciter la loi de groupe : si T_1 et T_2 sont deux torseurs sous A et si l'on fait agir A sur le produit $T_1 \times T_2$ par $(x, y) + a = (x + a, y - a)$, le quotient de $T_1 \times T_2$ par cette action est encore un torseur sous A, et sa classe dans $H^1(G, A(\overline{k}))$ est la somme des classes de T_1 et T_2. Notons $Ш(A/k)$ le sous-groupe de $H^1(G, A(\overline{k}))$ constitué des classes de torseurs possédant un point k_v-rationnel pour toute place v de k : c'est le *groupe de Tate-Shafarévitch de A sur k*. Tautologiquement, une courbe projective et lisse de genre 1 vérifie le principe de Hasse si et seulement si sa classe dans le groupe de Tate-Shafarévitch de sa jacobienne est nulle.

Proposition — *Soit A une variété abélienne sur un corps de nombres k. Le groupe $Ш(A/k)$ est de torsion et sa m-torsion est finie pour tout $m \in \mathbb{N}^\star$.*

Il existe une notion de dualité des variétés abéliennes ; tout ce qu'il faut savoir est qu'en dimension 1, la dualité est triviale, i.e. une courbe elliptique est canoniquement isomorphe à sa duale. Notons $\hat{A}$ la variété abélienne duale de A. On dispose d'une application $\mathbb{Z}$-bilinéaire

$$Ш(A/k) \times Ш(\hat{A}/k) \longrightarrow \mathbb{Q}/\mathbb{Z},$$

appelée *accouplement de Cassels-Tate*. Lorsque A est une courbe elliptique et que l'on identifie $\hat{A}$ à A de la manière canonique, cet accouplement est alterné. De plus, il est non dégénéré si $Ш(A/k)$ est fini ; par conséquent, lorsque $\dim A = 1$, l'ordre de $Ш(A/k)$ est un carré s'il est fini.

Conjecture — *Soit A une variété abélienne sur un corps de nombres k. Le groupe $Ш(A/k)$ est fini.*

Même dans le cas d'une courbe elliptique sur $\mathbb{Q}$, cette conjecture est loin d'être démontrée. Son intérêt premier est le suivant : si $Ш(A/k)$ est fini, il existe un algorithme (dit de descente) permettant de déterminer un système de générateurs du groupe abélien de type fini $A(k)$ (plus précisément, on dispose d'un algorithme mais il peut entrer dans une boucle infinie si $Ш(A/k)$ possède un élément infiniment divisible).

Résumons ce que l'on sait sur la possibilité de déterminer algorithmiquement l'ensemble des points rationnels d'une courbe projective et lisse C sur un corps de nombres k.

1. Si C est de genre 0 : il existe un algorithme. Si l'on trouve un point rationnel sur C, on peut les paramétrer tous par $\mathbb{P}^1(k)$ et de manière explicite, comme on l'a vu dans la section précédente. Il suffit donc de savoir décider l'existence d'un point rationnel. Comme C satisfait le principe de Hasse, on peut se ramener à un corps local, puis à des quotients finis de son anneau des entiers, où l'on peut tester toutes les possibilités.
2. Si C est de genre 1 : il existe un algorithme si le groupe de Tate-Shafarévitch de la jacobienne de C est fini. Notons E la jacobienne de C. Si $C(k) \neq \varnothing$, on peut trouver un point rationnel par inspection. Ce point fournit un isomorphisme entre C et E, de sorte qu'il ne reste plus qu'à appliquer l'algorithme de

descente afin de déterminer les points rationnels de C. Si $C(k) = \varnothing$, la classe de C dans $Ш(E/k)$ est non nulle ; comme l'accouplement de Cassels-Tate est non dégénéré, il suffit pour le prouver d'expliciter une classe de $Ш(E/k)$ qui n'est pas orthogonale à C, ce que l'on peut faire par inspection.

3. Si C est de genre supérieur ou égal à 2 : la réponse n'est pas connue. On s'attend cependant à ce qu'elle soit positive.

3.3 Obstruction de Brauer-Manin

La théorie de la cohomologie étale permet de généraliser la notion de groupe de Brauer d'un corps aux variétés algébriques. Rappelons que si k est un corps, $\overline{k}$ une clôture séparable de k et G le groupe de Galois de $\overline{k}$ sur k, $\mathrm{Br}(k)$ est égal à $H^2(G, \overline{k}^\star)$. Cohomologie étale de la variété sur k réduite à un point et cohomologie galoisienne de k coïncident ; il est donc naturel d'appeler groupe de Brauer d'une variété algébrique projective V sur k le groupe $H^2_{\text{ét}}(V, \mathbb{G}_{\mathrm{m}})$, où $\mathbb{G}_{\mathrm{m}}$ désigne le groupe multiplicatif sur V. À nouveau, $\mathrm{Br}(V)$ est fonctoriel en V. Notamment, si x est un point K-rationnel de V, on peut évaluer un élément A de $\mathrm{Br}(V)$ en x, et l'on obtient ainsi un élément $A(x)$ de $\mathrm{Br}(K)$. Si k est un corps de nombres, pour tout $A \in \mathrm{Br}(V)$, il existe un ensemble fini S de places de k tel que pour toute place $v \notin S$ et tout $x \in V(k_v)$, on ait $A(x) = 0$.

Proposition — *Soit X une variété projective et lisse sur un corps de nombres k. Si pour toute famille $(P_v)_v$ de $\prod_v X(k_v)$, il existe un $A \in \mathrm{Br}(X)$ tel que $\sum_v \mathrm{inv}_v(A(P_v)) \neq 0$, alors $X(k) = \varnothing$.*

Démonstration — C'est une conséquence immédiate de la suite exacte (2). Notons que l'on ne se sert que de la nullité de la composée des flèches. □

Si B est un sous-groupe de $\mathrm{Br}(X)$ tel que pour tout $(P_v)_v \in \prod_v X(k_v)$, il existe $A \in B$ tel que $\sum_v \mathrm{inv}_v(A(P_v)) \neq 0$, on dit que B fournit une *obstruction de Brauer-Manin* au principe de Hasse. Dans la pratique, B est souvent cyclique.

Définition — *Soit $\mathscr{V}$ une classe de variétés algébriques projectives et lisses sur un corps de nombres k. On dit que l'obstruction de Brauer-Manin au principe de Hasse est la seule pour $\mathscr{V}$ si tout $X \in \mathscr{V}$ tel qu'il existe une famille $(P_v)_v \in \prod_v X(k_v)$ vérifiant*

$$\forall A \in \mathrm{Br}(X),\ \sum_v \mathrm{inv}_v(A(P_v)) = 0$$

possède un point rationnel.

L'obstruction de Brauer-Manin permet d'expliquer la plupart des exemples connus de variétés ne vérifiant pas le principe de Hasse. Une nouvelle question apparaît naturellement : trouver des classes de variétés pour lesquelles l'obstruction de Brauer-Manin au principe de Hasse est la seule. Il est conjecturé que la classe des variétés rationnelles convient (une variété est dite *rationnelle* si, après extension des scalaires de k à $\overline{k}$, son corps de fonctions rationnelles est une extension purement transcendante de $\overline{k}$). Pour les courbes de genre 1, on dispose du résultat suivant.

Théorème (Manin) — *Sous l'hypothèse de la finitude des groupes de Tate-Shafarévitch des courbes elliptiques sur k, l'obstruction de Brauer-Manin au principe de Hasse est la seule pour les courbes projectives et lisses de genre 1 sur k.*

4 Conjecture de Tate et cycles algébriques

Soient C une courbe projective et lisse sur un corps fini k, K le corps de ses fonctions rationnelles, $\overline{K}$ une clôture séparable de K, G le groupe de Galois de $\overline{K}$ sur K et A une variété abélienne sur K. Par analogie avec la situation sur un corps de nombres, on définit le groupe de Tate-Shafarévitch $Ш(A/K)$ comme étant le sous-groupe de $H^1(G, A(\overline{K}))$ constitué des classes de torseurs possédant un point K_v-rationnel pour tout

$v \in C$, en notant K_v le complété de K par rapport à la valuation définie par v (à une fonction rationnelle f sur C, elle associe son ordre d'annulation en v).

Considérons le cas où A est la jacobienne de la fibre générique d'un morphisme $f\colon X \to C$, où X est une surface projective et lisse sur k. Pour être rigoureux, on suppose que f est plat, admet une section et que ses fibres sont géométriquement connexes. Des considérations sur le foncteur de Picard relatif de X sur C permettent de prouver, à l'aide de la suite spectrale de Leray pour f et le faisceau étale $\mathbb{G}_{\mathrm{m}}$, que l'on a alors un isomorphisme canonique $\mathrm{Br}(X) = Ш(A/K)$. La question sur la finitude du groupe de Tate-Shafarévitch nous amène donc naturellement à la conjecture suivante.

Conjecture (Tate) — *Le groupe de Brauer d'une variété projective et lisse sur un corps fini est fini.*

Le résultat est connu pour les courbes (le groupe de Brauer est même nul, dans ce cas), pour les variétés abéliennes, pour certaines surfaces $K3$, pour certaines variétés de Fermat (i.e. les hypersurfaces projectives définies par une équation de la forme $x_0^m + \cdots + x_n^m = 0$), et pour les produits de telles variétés.

Cette conjecture peut se reformuler en termes de cohomologie ℓ-adique. Soit X une variété projective et lisse sur un corps k de caractéristique p éventuellement nulle. Notons $\overline{k}$ une clôture séparable de k, G le groupe de Galois de $\overline{k}$ sur k et $X_{\overline{k}}$ la variété sur $\overline{k}$ déduite de X par extension des scalaires. Choisissons un nombre premier $\ell \neq p$. Les groupes de cohomologie ℓ-adique de X se notent $H^i(X_{\overline{k}}, \mathbb{Q}_\ell)$ et sont nuls pour $i > 2 \dim X$; il faut y penser comme à des groupes de cohomologie singulière. Lorsque $\overline{k} = \mathbb{C}$, la cohomologie singulière à coefficients dans $\mathbb{Q}_\ell$ de l'espace topologique $X(\mathbb{C})$ coïncide d'ailleurs avec la cohomologie ℓ-adique de X. Cette dernière est cependant plus riche, car G agit sur $H^i(X_{\overline{k}}, \mathbb{Q}_\ell)$. Un *diviseur* sur X, ou *cycle algébrique de codimension* 1, est une combinaison $\mathbb{Z}$-linéaire formelle de sous-variétés projectives irréductibles de X de codimension 1. De même qu'en cohomologie singulière, on peut associer une classe dans $H^2(X_{\overline{k}}, \mathbb{Q}_\ell)$ à un diviseur sur X (intuitivement, on arrive dans la cohomologie de degré 2 car une sous-variété de codimension algébrique 1 est de codimension « topologique » 2 — penser aux points complexes lorsque $\overline{k} = \mathbb{C}$). Cette association n'est canonique et G-équivariante que si l'on tord le groupe de cohomologie par le caractère cyclotomique ; le groupe obtenu se note $H^2(X_{\overline{k}}, \mathbb{Q}_\ell(1))$. On obtient donc une application $\mathbb{Q}_\ell$-linéaire

$$\mathrm{Div}(X) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \xrightarrow{\rho} H^2(X_{\overline{k}}, \mathbb{Q}_\ell(1))^G,$$

en notant $\mathrm{Div}(X)$ le groupe des diviseurs sur X.

Conjecture (Tate) — *Si k est de type fini sur son sous-corps premier, l'application ρ est surjective.*

Lorsque k est fini, on peut montrer que ces deux conjectures sont équivalentes. Ainsi, ce dernier énoncé est relié à des questions sur le principe de Hasse pour des courbes projectives et lisses de genre 1. Pour terminer, mentionnons un fait en apparence plus surprenant : l'essentiel de la preuve du théorème de Faltings sur les courbes de genre au moins 2, sur un corps de nombres, consiste à montrer la validité de la conjecture de Tate lorsque X est une variété abélienne...