J.-L. Colliot-Thélène (CNRS et Université Paris-Sud)

Groupe de Brauer et obstruction de Brauer-Manin

École d'été de Yaroslav

25 juillet-30 juillet 2012

Congruences, corps locaux

Soit $f(x_1, \cdots, x_n)$ un polynôme à coefficients entiers.
On cherche des méthodes pour décider si une équation

$$f(x_1, \cdots, x_n) = 0$$

a des solutions entières.

Si f est homogène, on s'intéresse aux solutions primitives (entiers x_i premiers entre eux dans leur ensemble).

Il est parfois facile de décider qu'il n'y a pas de solutions.
Ainsi $x^2 + y^2 + 1 = 0$ n'a pas de solution dans $\mathbb{R}$, donc pas dans $\mathbb{Z}$.
On peut aussi utiliser des congruences pour voir qu'il n'y a pas de solutions.
Avec des congruences modulo 9 on voit que l'équation $x^2 + y^2 - 3z^2 = 0$ n'a pas de solution non triviale. On peut aussi le voir par des congruences modulo 4.
Soit p un nombre premier. Avec des congruences modulo p^3 on voit que l'équation

$$x^3 + py^3 + p^2z^3 = 0$$

n'a pas de solution non triviale.

Problème local-global : Si les conditions de congruence sont satisfaites modulo tout entier (et s'il y a des solutions réelles), y a-t-il des solutions entières ?

Problème d'approximation : Si toutes les conditions de congruence (et de réalité) sont satisfaites, si l'on se donne un entier $m > 0$ et $(b_1, \ldots, b_n) \in \mathbb{Z}^n$ avec

$$f(b_1, \cdots, b_n) = 0 \mod m$$

existe-t-il $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ congru à $(b_1, \ldots, b_n)$ modulo m tel que

$$f(a_1, \cdots, a_n) = 0 \, ?$$

On doit à Kurt Hensel l'invention des corps locaux. A tout premier p on associe un anneau intègre $\mathbb{Z}_p$. Son corps des fractions $\mathbb{Q}_p$ est la complétion de $\mathbb{Q}$ par rapport à la métrique p-adique définie par

$$|p^n \cdot a/b|_p = 1/p^n$$

($a, b \in \mathbb{Z}$, a et b premiers à p.)
Une équation $f(x_1, \cdots, x_n) = 0$ à coefficients entiers a une solution (primitive) dans $\mathbb{Z}_p$ si et seulement si elle a une solution (primitive) modulo une puissance arbitraire de p.

Soit $X(R)$ l'ensemble des solutions de l'équation $f(x_1, \cdots, x_n) = 0$ à coordonnées dans l'anneau commutatif R. Les inclusions

$$X(\mathbb{Z}) \subset \prod_p X(\mathbb{Z}_p) \subset X(A_{\mathbb{Q}})$$

$$X(\mathbb{Q}) \subset X(A_{\mathbb{Q}}) \subset \prod_p X(\mathbb{Q}_p)$$

résument toutes les conditions de congruence (et de réalité).
Ici p est un premier ou $p = \infty$, dans ce dernier cas on pose $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$. L'ensemble $X(A_{\mathbb{Q}})$, l'espace des adèles, est formé des solutions à coefficients entiers pour presque tout premier p.

Le théorème de Legendre

Théorème (Legendre, 1785) *Soit $q(x, y, z)$ une forme quadratique entière. Si l'équation $q(x, y, z) = 0$ a une solution non triviale dans chaque $\mathbb{Z}_p$, y compris $\mathbb{R}$, alors elle a une solution non triviale dans $\mathbb{Z}$.*

La démonstration relève de la géométrie des nombres. Elle donne une borne supérieure pour la taille de la plus petite solution.

Les diverses démonstrations n'utilisent pas toute l'hypothèse ; on peut par exemple omettre l'hypothèse $X(\mathbb{R}) \neq \emptyset$. Ainsi cette condition est imposée par l'hypothèse $X(\mathbb{Z}_p) \neq \emptyset$ pour p fini. Ce fait curieux est un cas particulier d'une loi de réciprocité.

La loi de réciprocité quadratique

Soit $p \neq 2$ un premier impair, $a \in \mathbb{Z}$ premier à p,
Le symbole de Legendre $(a/p) = \pm 1$ est défini par :
$(a/p) = 1$ si et seulement si a est un carré mod. p.

Soient p, q des premiers impairs. Alors

$$(p/q)(q/p) = (-1)^{(p-1)/2.(q-1)/2}$$

Ceci fut conjecturé indépendamment par Euler et Legendre (1785).
La première d'une série de démonstrations fut trouvée par Gauß le 18 avril 1796.

Soit p un premier impair.
Première loi complémentaire

$$(-1/p) = (-1)^{(p-1)/2}$$

Ainsi : -1 est un carré modulo p si et seulement si $p \equiv 1(4)$.

Deuxième loi complémentaire

$$(2/p) = (-1)^{(p^2-1)/8}$$

Ainsi : 2 est un carré modulo p si et seulement si $p \equiv \pm 1(8)$.

Le principe de Hasse pour les formes quadratiques

Théorème (Minkowski; Hasse 1920) *Soit* $n \geq 2$. *Let* $q(x_1, \cdots, x_n)$ *une forme quadratique entière. Si l'équation*

$$q(x_1, \cdots, x_n) = 0$$

a des solutions non triviales dans tous les $\mathbb{Z}_p$ *y compris* $\mathbb{R}$, *alors elle a une solution non triviale dans* $\mathbb{Z}$.
L'argument principal dans la démonstration de Hasse se situe au passage de 3 variables (Legendre) à 4 variables. Hasse combine le théorème de Dirichlet sur les nombres premiers dans une progression arithmétique avec la loi de réciprocité.

Voici quelques théorèmes célèbres que l'on peut considérer comme des principes locaux globaux pour les solutions en entiers des équations à coefficients entiers.

Tout premier p congru à 1 modulo 4 est une somme de deux carrés (Fermat).

L'équation $n = x^2 + y^2 + z^2$ pour n entier a une solution en entiers si elle a une solution sur $\mathbf{R}$ et sur $\mathbb{Z}_2$ (c'est-à-dire $n > 0$ et $n \neq 4^r(8m + 7)$) (Legendre, Gauß)

L'équation $n = x^2 + y^2 + z^2 + t^2$ pour n entier a une solution en entiers si $n > 0$ (Lagrange)

Question de base : **Y a-t-il un tel théorème local-global, ou un substitut, pour d'autres familles d'équations ?**
On parle alors de "principe de Hasse".
Voici des résultats classiques dans ce sens.

Pour les points rationnels :

Les variétés projectives espaces homogènes de groupes algébriques linéaires connexes (mélange de théorie du corps de classes et de théorie des groupes algébriques linéaires, Eichler, Kneser, Harder).

Hypersurfaces projectives $F_d(x_0, \cdots, x_n) = 0$ avec n grand par rapport à d : méthode du cercle.

Pour les points entiers :

Représentation d'un entier par une forme quadratique entière *indéfinie* en au moins 4 variables (Eichler, Kneser)

Représentation d'un entier par certaines formes $F_d(x_0, \cdots, x_n)$ à coefficients entiers, avec n grand par rapport au degré d (problème de Waring, méthode du cercle).

Exercice. Établir le principe de Hasse pour tout système d'équations

$$q_1(x_1, y_1) = \cdots = q_n(x_n, y_n) \neq 0$$

où les $q_i(x_i, y_i)$ sont des formes quadratiques binaires non dégénérées à coefficients dans $\mathbb{Q}$.

Idée : copier la démonstation de Hasse du principe pour les formes quadratiques à 4 variables à partir de celui pour les formes à 3 variables.

Pour les exercices suivants, copier le passage de 4 à 5 variables dans la preuve du principe de Hasse pour les formes quadratiques.

– Montrer que le principe de Hasse pour les points rationnels vaut pour toute équation

$$\sum_{i=1}^{3} a_i x_i^2 = P(x_4) \neq 0,$$

avec les $a_i \in \mathbb{Q}^\times$ et $P(t) \neq 0$ un polynôme.

– Montrer que le principe de Hasse pour les points rationnels vaut pour

$$\sum_{i=1}^{4} a_i(t) x_i^2 = a_5(t) \neq 0$$

où les $a_i(t)$ sont des polynômes non nuls.

Contre-exemples au “principe de Hasse” pour les points rationnels

Exemples de Hasse et Witt, 1934

Equation $\mathrm{Norm}_{K/\mathbb{Q}}(x) = c$ avec $K/\mathbb{Q}$ extension galoisienne convenable de groupe $\mathbb{Z}/2 \times \mathbb{Z}/2$. Un peu délicat.

Exemple $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, $c = 5^2, 7^2, 10^2, 11^2, 14^2$. Voir Cassels–Fröhlich p. 360. Ou récente note (CT).

L'exemple de Lind (1940)
Il y a une courbe de genre 1 sur $\mathbb{Q}$ qui a des points dans tous les $\mathbb{Q}_p$ et $\mathbb{R}$, et qui n'a pas de point dans $\mathbb{Q}$.

$$2y^2 = x^4 - 17, \quad x, y \in \mathbb{Q}$$

$$2u^2 = v^4 - 17w^4 \neq 0, \quad u, v, w \in \mathbb{Z}, \quad (v, w) = 1$$

Par réduction modulo 17^2, on voit que u n'est pas divisible par 17. Comme 2 n'est pas une puissance quatrième modulo 17, ceci implique : *u n'est pas un carré modulo 17*.

Si p est un premier impair qui divise u (et donc $p \neq 17$), alors 17 est un carré modulo p, donc (loi de réciprocité quadratique) p est un carré modulo 17. Puisque 2 est aussi un carré modulo 17, on conclut : *u est un carré modulo 17*.
Contradiction, $X(\mathbb{Q}) = \emptyset$.

L'exemple d'Iskovskikh (1971)

C'est une surface (géométriquement) "rationnelle", famille à un paramètre de coniques, qui a des points dans tous les $\mathbb{Q}_p$ et dans $\mathbb{R}$ mais qui n'a pas de points dans $\mathbb{Q}$.

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

Solution avec $x, y, z \in \mathbb{Q}$?

$$u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0,$$

avec $u, v, x, y \in \mathbb{Z}, (x, y) = 1$, donc $(3y^2 - x^2, x^2 - 2y^2) = 1$

Modulo 4, le couple $(3y^2 - x^2, x^2 - 2y^2)$ prend l'une des valeurs suivantes :

$$(2, -1), (-1, 1), (3, 2)$$

Dans $\mathbb{R}$ on a $3y^2 - x^2 > 0, \;\; x^2 - 2y^2 > 0.$

$$u^2 + v^2 = (3y^2 - x^2)(x^2 - 2y^2) \neq 0,$$

Soit p un premier impair. Si p^{2n+1} divise exactement soit $3y^2 - x^2$ soit $x^2 - 2y^2$, alors p^{2n+1} divise exactement $u^2 + v^2$, ainsi -1 is est un carré mod. p, donc (première loi complémentaire) $p \equiv 1$ mod. 4.
Ainsi le couple $(3y^2 - x^2, x^2 - 2y^2)$ prend l'une des valeurs suivantes modulo 4 :

$$(1, 1), (2, 1), (1, 2)$$

donc aucune des précédentes valeurs

$$(2, -1), (-1, 1), (3, 2)$$

Contradiction, $X(\mathbb{Q}) = \emptyset$.

Exercice. Généraliser à $y^2 + z^2 = (c - x^2)(x^2 - c + 1)$ avec $c > 0$ congru à 3 modulo 4.

Exercice (Swinnerton-Dyer, 1961). Montrer que pour la surface X définie par $y^2 + z^2 = (4x - 7)(x^2 - 2)$ le lieu réel $X(\mathbb{R})$ a deux composantes connexes, $x \geq 7/4$ et $-\sqrt{2} \leq x \leq \sqrt{2}$, et qu'il n'y a pas de point de $X(\mathbb{Q})$ dans la seconde composante ("défaut d'approximation faible").

Exemples (plus délicats) non discutés en détail ici :

$3x^3 + 4y^3 + 5z^3 = 0$ (Selmer)

$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$ (Cassels-Guy, 1966)

Nombreux exemples pour

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

avec $a, b, c, d \in \mathbb{Z}$, sans facteur cubique.
Conjecture (CT-Kanevsky-Sansuc) : S'il existe un nombre premier p qui ne divise qu'un seul des a, b, c, d, alors le principe de Hasse vaut pour une telle équation.

Contre-exemples au principe de Hasse pour les points entiers

Équations

$$q(x, y) = a$$

$$q(x, y, z) = a$$

avec q forme quadratique à coefficients entiers

Il y a des solutions dans tous les $\mathbb{Z}_p$ et $\mathbb{R}$ mais pas de solutions dans $\mathbb{Z}$ pour :
L'équation $23 = x(x + 7y)$
Le système d'équations $\{2x - 5y = 1, xt = 1\}$
L'équation $1 = 4x^2 + 25y^2$
(Arguments élémentaires)

L'équation $1 = 4x^2 - 475y^2$ (plus difficile !)

(Sur $\mathbb{Q}$, ces courbes sont le complément dans $\mathbb{P}^1_{\mathbb{Q}}$ de deux points, rationnels ou quadratiques conjugués.)

Pour q premier, l'équation $q = x^2 + 27y^2$
a des solutions dans tous les $\mathbb{Z}_p$ si et seulement si $q \equiv 1 \bmod 3$
Si c'est le cas, elle a une solution dans $\mathbb{Z}$ si et seulement si 2 est un cube dans $\mathbf{F}_q$ (condition a priori mystérieuse).

Euler, Gauß, voir le livre de D. Cox sur $p = x^2 + ny^2$.

Schulze-Pillot et Xu

Soit $X_{n,m}$ with $n, m \in \mathbb{N}$, $(n, m) = 1$ donné par

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

Alors $X_{n,m}(\mathbb{Z}_p) \neq \emptyset$ pour tout premier p.
$X_{n,m}(\mathbb{Z}) = \emptyset$ si
– soit 2 divise exactement m et $n \equiv 5 \bmod 8$
– soit 4 divise m et $n \equiv \pm 3 \bmod 8$.

Théorème (Schulze-Pillot et Xu). Dans les autres cas, $X_{n,m}(\mathbb{Z}) \neq \emptyset$.

Borovoi et Rudnick, 1995

Considérons l'équation sur $\mathbb{Z}$:

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

soit

$$(x - y)^2 + 8(x - y)(x + y) = 2z^2 - 1$$

Solution dans $\mathbb{Q}$

$$(x, y, z) = (-1/2, 1/2, 1)$$

donc solutions dans tous les $\mathbb{Z}_p$ pour $p \neq 2$.

Solution dans $\mathbb{Z}_2$, en utilisant $q(4, 1, 1) = -127 \equiv 1(8)$.

$$(x-y)^2 + 8(x-y)(x+y) = 2z^2 - 1$$

Solution avec $(x, y, z) \in \mathbb{Z}$?
Si on étudie l'équation modulo des puissances de 2, on trouve

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

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

On voit que dans beaucoup des contre-exemples décrits un instrument-clé est la loi de réciprocité quadratique.

On veut comprendre quelle est l'algèbre des équations considérées qui permet de faire les calculs.

Dans les exposés on se concentrera sur la question de l'existence de points rationnels et de points entiers sur les variétés de l'un des types suivants :
Espaces homogènes de groupes algébriques linéaires connexes
Espace total de familles à un paramètre de tels espaces

Les techniques expliquées ici sont aussi été utilisées dans l'étude des points rationnels des courbes de genre quelconque, dans celles des surfaces géométriquement rationnelles, des surfaces K3, des surfaces d'Enriques.

Préliminaires de géométrie algébrique; le groupe de Picard

Soit A un anneau commutatif unitaire. On note $X = \mathrm{Spec}A$ son spectre, c'est-dire l'ensembles des idéaux premiers de A. On a la topologie de Zariski sur $\mathrm{Spec}A$, une base d'ouverts étant formée des $X_f = \mathrm{Spec}A[1/f]$ pour $f \in A$ non diviseur de zéro. On a sur X un faisceau d'anneaux donné par les $A[1/f]$ sur X_f.
Un schéma X est un espace topologique, muni d'un faisceau d'anneaux commutatifs, qui admet une base d'ouverts des schémas affines comme ci-dessus.
Il est donc obtenu par recollement d'espaces affines.
Exemple : droite projective $\mathbb{P}^1_k$, recollée de $\mathrm{Spec}k[t]$ et de $\mathrm{Spec}k[1/t]$.

Un anneau noethérien A est dit de valuation discrète s'il est intègre, local, et l'idéal maximal est engendré par un élément. Le corps des fractions K est alors muni d'une valuation discrète c'est-à-dire d'un homomorphisme $v : K^{\times} \to \mathbb{Z}$ satisfaisant

$$v(x+y) \geq inf(v(x), v(y)$$

avec égalité si $v(x) \neq v(y)$. On a

$$A = \{x \in K, v(x) \geq 0\}$$

$$m = \{x \in K, v(x) \geq 1.\}$$

Exemple d'anneau de valuation discrète : localisé $\mathbb{Z}_{(p)}$ de $\mathbb{Z}$ en un premier p.
Un anneau de Dedekind est un anneau noethérien dont les localisés A_p sont des anneaux de valuation discrète ou des corps.
Exemples :
anneau des entiers d'un corps de nombres, et tout localisé d'un tel anneau.
pour K une extension finie séparable de $k(t)$, la clôture intégrale de $k[t]$ dans K.

Étant donné un anneau commutatif A noethérien, un A-schéma de type fini est un schéma X qui admet un recouvrement ouvert fini par des schémas $\mathrm{Spec}B$ avec B une A-algèbre de type fini, c'est-à-dire engendrée par un nombre fini d'éléments.
On s'intéresse alors à l'ensemble $X(A)$ de ses "A$-$*points*".
On s'intéressera particulièrement au cas où A est un corps k ("variétés", k-variétés), dans ce cas $X(k)$ est l'ensemble des points rationnels.
On s'intéressera aussi au cas où A est un anneau de valuation discrète ou un anneau Dedekind ("schémas arithmétiques"), dans ce cas $X(A)$ est l'ensemble des points "entiers".

Propriétés intéressantes des anneaux noethériens inègres (= sans diviseur de zéro).
Anneau normal : intégralement clos dans son corps des fractions K
Pour un tel anneau, le lcoalisé A_p d'un tel anneau en un idéal premier de hauteur 1 est un anneau de valuation discrète, on note $v_p : K^\times \to \mathbb{Z}$ la valuation associée. On a $A = \bigcap_{p,ht(p)=1} A_p \subset K$.
Anneau factoriel : tout idéal premier de hauteur 1 est principal. Un tel anneau est normal.
Anneau localement factoriel : tous les localisés A_p sont factoriels.
Anneau local régulier : idéal maximal engendré par $dim(A)$ éléments. Tout tel anneau est factoriel (Auslander-Buchsbaum-Serre).
Anneau régulier : les localisés sont réguliers.

Propriétés globales des k-variétés (k un corps)

k-variété lisse : localement donnée par un système fini de polynômes satisfaisant le critère jacobien.
Par exemple $f(x, y) = 0$, avec f, f'_x, f'_y sans zéro commun sur une clôture algébrique de k.
Une k-variété lisse est un schéma régulier.

k-variété projective, donnée par un nombre fini d'équations homogènes dans un espace projectif.
Analogue $X \subset \mathbb{P}^n_A$ sur A anneau de valuation discrète de corps des fractions K. On a alors la "propreté" de X sur A :

$$X(A) = X(K).$$

Étant donné un schéma X, on a le faisceau d'anneaux O_X et donc le faisceau de groupes multiplicatifs $O_X^\times$.
On définit

$$\mathrm{Pic}(X) = H^1_{Zar}(X, O_X^\times).$$

Pour tout morphisme de schémas $X \to Y$ on a une flèche fonctorielle induite $\mathrm{Pic}(Y) \to \mathrm{Pic}(X)$.

Étant donné un schéma intègre son corps des fonctions est le "corps des fonctions rationnelles sur X", on le note K_X, il définit un faisceau constant sur X, le quotient de l'inclusion $O_X^\times \to K_X^\times$ définit le faisceau des diviseurs de Cartier sur X (sous-variétés définies localement par une équation).

Supposons X noethérien régulier. Alors
diviseurs de Cartier = diviseurs de Weil,
on a une suite exacte de faisceaux

$$1 \to O_X^\times \to K_X^\times \to \oplus_{x \in X^1} \mathbb{Z}_x \to 0,$$

où $\mathbb{Z}_x$ est le faisceau constant $\mathbb{Z}$ sur le point x de codimension 1, et la flèche $K_X^\times \to \mathbb{Z}_x$ associe à une fonction sa valuation dans l'anneau local $O_{X,x}$, qui est de valuation discrète : c'est l'ordre du pôle ou du zéro de la fonction le long de la sous-variété de codimension 1 associée.
Notant $WDiv(X) = \oplus_{x \in X^1} \mathbb{Z}$, on a alors une suite exacte de groupes

$$1 \to \Gamma(X, O_X^\times) \to K_X^\times \to WDiv(X) \to \mathrm{Pic}(X) \to 0.$$

Suite de localisation. Soit U ouvert non vide de X une k-variété lisse intègre. Il y a un ensemble T fini de points de codimension 1 dans $X \setminus U$. On a la suite exacte

$$1 \to k[X]^\times \to k[U]^\times \to \oplus_{x \in T} \mathbb{Z} \to \mathrm{Pic}(X) \to \mathrm{Pic}(U) \to 0.$$

Ainsi $\mathrm{Pic}(X)$ est de type fini comme groupe abélien si et seulement si il existe un ouvert non vide $U \subset X$ avec $\mathrm{Pic}(U) = 0$.

Exercices.

Soit k un corps.

1. Montrer $\mathrm{Pic}(\mathbb{A}^n_k) = 0$.
2. Montrer $\mathrm{Pic}(\mathbb{P}^n_k) = \mathbb{Z}H$, avec H la classe d'un hyperplan.
3. Montrer que si X/k est lisse alors $\mathrm{Pic}(X \times_k \mathbb{P}^n_k) \simeq \mathrm{Pic}(X) \oplus \mathbb{Z}$.
4. Soit $X \subset \mathbb{P}^3_k$ la quadrique $xy - zt = 0$. Montrer $\mathrm{Pic}(X) = \mathbb{Z} \oplus \mathbb{Z}$.
5. Soit $X \subset \mathbb{P}^n_k$ une quadrique lisse donnée par $x_0x_1 + \sum_{i=2}^n a_i x_i^2 = 0$. Montrer $\mathrm{Pic}(X) = \mathbb{Z}H$, avec H la classe d'une section hyperplane. Montrer que pour Y affine donnée par $xy - zt = 1$ on a $\mathrm{Pic}(Y) = 0$. Montrer que Y n'est pas isomorphe à l'espace affine $\mathbb{A}^3_k$.

Pour X/k et Y/k projectifs lisses intègres, les propriétés suivantes sont équivalentes :
(a) Les corps de fonctions $k(X)$ et $k(Y)$ sont k-isomorphes.
(b) Il existe des ouverts non vides $U \subset X$ et $V \subset Y$ qui sont k-isomorphes.
On dit que X et Y sont k-birationnelles.

Exercice. Montrer qu'alors il existe des entiers $r, s \geq 0$ tels que

$$\mathrm{Pic}(X) \oplus \mathbb{Z}^r \simeq \mathrm{Pic}(Y) \oplus \mathbb{Z}^s.$$

On dit que la k-variété intègre X est k-unirationnelle s'il existe un k-plongement $k(X) \subset k(\mathbb{A}^n)$. Pour X/k projective lisse et $car(k) = 0$ ceci implique que $\mathrm{Pic}(X)$ est un groupe abélien libre de type fini.

À une variété X/k projective, lisse, géométriquement intègre sur un corps k, on associe sa k-variété de Picard $\mathrm{Pic}^0_{X/k}$. C'est une variété abélienne (projective et munie d'une structure de groupe). Si k est de caractéristique zéro, sa dimension est égale à la dimension du k-vectoriel de dimension finie $H^1(X, O_X)$.
On a une suite exacte de modules galoisiens

$$0 \to \mathrm{Pic}^0_{X/k}(\overline{k}) \to \mathrm{Pic}(\overline{X}) \to NS(\overline{X}) \to 0,$$

où $NS(\overline{X})$ est un groupe abélien de type fini, le groupe de Néron-Severi de $\overline{X}$.
Pour une courbe, $NS(\overline{X}) = \mathbb{Z}$, la flèche $\mathrm{Pic}(\overline{X}) \to NS(\overline{X}) = \mathbb{Z}$ est donnée par le degré des diviseurs.

Un peu de cohomologie galoisienne

(voir le cours de Kunyavskiĭ l'an dernier)

Soit G un groupe fini. À tout G-module A (groupe abélien équipé d'une action d'un groupe fini G), on associe le sous-groupe des invariants $A^G \subset A$.
Si l'on a une suite exacte de G-modules

$$1 \to A \to B \to C \to 0$$

on voit facilement que cela induit une suite exacte

$$0 \to A^G \to B^G \to C^G$$

mais la flèche $B^G \to C^G$ n'est pas forcément surjective.

L'algèbre homologique associe à tout G-module A des groupes abéliens $H^i(G, A)$ $(i \geq 0)$ de façon fonctorielle en A, de telle façon que $H^0(G, A)$ et qu'une suite exacte comme ci-dessus donne naissance à une suite exacte infinie

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B)$$

$$\to H^1(G, C) \to H^2(G, A) \to H^2(G, B) \to \cdots$$

Les groupes $H^i(G, A)$ se décrivent simplement comme quotients de groupes de "cocycles" par des sous-groupes de "cobords".
On a une théorie analogue quand on considère un groupe g profini (limite inverse de groupes finis, comme le groupe de Galois absolu d'un corps), équipé de sa topologie naturelle de groupe compact, et des g-modules continus discrets (le stabilisateur de tout point est ouvert dans le groupe g).
Pour le groupe de Galois absolu $G_k = Gal(\overline{k}/k)$ d'un corps k, on note souvent $H^i(k, A) = H^i(G_k, A)$.

Les groupes $H^i(G, A)$ pour $i \geq 1$ sont de torsion, annulés par l'ordre de G si G est fini. En particulier si A est un $\mathbb{Q}$-vectoriel, $H^i(G, A) = 0$ pour $i \geq 1$.
Pour un G-module trivial A, on a $H^1(G, A) = Hom(G, A)$.
Pour tout G-réseau de permutation P (somme directe de $\mathbb{Z}[G/H]$) on a $H^1(G, P) = 0$.
La suite exacte de G-modules

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

donne naissance à des isomorphismes

$$H^i(G, \mathbb{Q}/\mathbb{Z}) \simeq H^{i+1}(G, \mathbb{Z})$$

($i \geq 1$). En particulier $Hom(G, \mathbb{Q}/\mathbb{Z}) \simeq H^2(G, \mathbb{Z})$.

Soit K/k une extension galoisienne de corps, de groupe de Galois G. Un théorème-clé est le théorème 90 de Hillbert, sous la forme d'Emmy Noether :

$$H^1(G, K^\times) = 0.$$

La version originelle de Hilbert est le cas K/k cyclique de groupe $G =< \sigma >$. Elle s'énonce : tout élément $x \in K^\times$ de norme $Norm_{K/k}(x) = 1$ s'écrit $x = \sigma(y)/y$ pour un $y \in K$.

Soit $\overline{k}$ une clôture séparable du corps k, et $g = Gal(\overline{k}/k)$.
On a $H^0(g, \overline{k}^\times) = k^\times$ et $H^1(g, \overline{k}^\times) = 0$.

Le groupe $H^2(g, \overline{k}^\times)$ est le **groupe de Brauer** $\mathrm{Br}(k)$ du corps k.

Ce groupe fut défini d'abord de façon non cohomologique par Richard Brauer. C'est le groupe des classes d'isomorphie d'agèbres centrales simples (de dimension finie) sur le corps k, pour l'addition définie par le produit tensoriel des algèbres, une fois passé au quotient par les classes d'algèbres de matrices.

Suite de Kummer

Pour tout entier $n > 0$ non nul dans k, l'élévation à la puissance n dans $\overline{k}^\times$ définit une suite exacte de modules galoisiens

$$1 \to \mu_n \to \overline{k}^\times \to \overline{k}^\times \to 1.$$

En utilisant le théorème 90 de Hilbert, on obtient

$$k^\times / k^{\times n} \simeq H^1(g, \mu_n)$$

et

$$H^2(g, \mu_n) \simeq \mathrm{Br}(k)[n].$$

($A[n] := \{x \in A, nx = 0\}$.)

Comportement du groupe de Picard par extension du corps de base

Soit X/k projective lisse géométriquement intègre et $\overline{X} = X \times_k \overline{k}$. On a $\overline{k}^\times = \overline{k}[X]^\times$. On peut considérer la suite exacte à 4 termes

$$1 \to \overline{k}^\times \to \overline{k}(X)^\times \to Div(\overline{X}) \to \mathrm{Pic}(\overline{X}) \to 0,$$

la couper en deux suites exactes courtes,

$$1 \to \overline{k}^\times \to \overline{k}(X)^\times \to \overline{k}(X)^\times/\overline{k}^\times \to 1$$

et

$$1 \to \overline{k}(X)^\times/\overline{k}^\times \to Div(\overline{X}) \to \mathrm{Pic}(\overline{X}) \to 0,$$

et considérer les suites exactes de cohomologie galoisienne associées.

En utilisant $H^1(g, \overline{k}^\times) = 0$, $H^1(g, \overline{k}(X)^\times) = 0$ (deux cas de Hilbert 90), puis $Div(X) = Div(\overline{X})^G$ (Cartier) et $H^1(g, Div(\overline{X})) = 0$ (Shapiro/Faddeev), on obtient facilement la suite exacte

$$0 \to \mathrm{Pic}(X) \to \mathrm{Pic}(\overline{X})^g \to H^2(g, \overline{k}^\times) \to H^2(g, \overline{k}(X)^\times)$$

et la suite exacte

$$0 \to H^1(g, \mathrm{Pic}(\overline{X})) \to H^2(g, \overline{k}(X)^\times / \overline{k}^\times) \to H^2(g, Div(\overline{X})).$$

On peut définir le "groupe de Brauer algébrique" d'une k-variété lisse X par la formule

$$\mathrm{Br}_{alg}(X) := Ker[H^2(g, \overline{k}(X)^\times) \to H^2(g, Div(\overline{X})].$$

On voit alors que l'on a une suite exacte

$$0 \to \mathrm{Br}_{alg}(X)/Im(\mathrm{Br}(k)) \to H^1(g, \mathrm{Pic}(\overline{X})) \to H^3(g, \overline{k}^\times).$$

En travaillant plus, on voit que sous l'hypothèse $X(k) \neq \emptyset$, on a $\mathrm{Pic}(X) \simeq \mathrm{Pic}(\overline{X})^g$ et $\mathrm{Br}_{alg}(X)/Im(\mathrm{Br}(k)) \simeq H^1(g, \mathrm{Pic}(\overline{X}))$.

Exercice. Soit $X \subset \mathbb{P}^2_k$ une conique lisse définie par $x^2 - ay^2 - bt^2 = 0$ ($car(k) \neq 2$). Montrer $\mathrm{Pic}(\overline{X})^g = \mathrm{Pic}(\overline{X}) = \mathbb{Z}$ engendré par la classe d'un point sur $\overline{k}$, et montrer que l'image d'une telle classe dans $H^2(g, \overline{k}^\times)$ est le groupe d'ordre au plus 2 engendré par la classe de l'algèbre de quaternions (a, b), et que l'on a une suite exacte

$$0 \to \mathbb{Z}/2(a, b) \to \mathrm{Br}(k) \to \mathrm{Br}_{alg}(X) \to 0.$$

Exercice. Soit $f(x, y, z, t)$ une forme quadratique non dégénérée sur k. Soit $d \in k^\times$ son discriminant. Soit $X \subset \mathbb{P}^3_k$ la quadrique lisse définie par $f = 0$. Alors :

(a) Il y a un isomorphisme de g-réseaux $\mathrm{Pic}(\overline{X}) \simeq \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$, avec l'action galoisienne suivante.
(b) Si $d \in k^{\times 2}$, l'action de g sur $\mathrm{Pic}(\overline{X})$ est triviale.
(c) Si $d \notin k^{\times 2}$, l'action de g se factorise à travers $\mathrm{Gal}(k(\sqrt{d})/k) \simeq \mathbb{Z}/2$, ce dernier groupe agissant par permutation de e_1 et e_2.
(d) La classe $e_1 + e_2$ appartient à $\mathrm{Pic}(X) \subset \mathrm{Pic}(\overline{X})$, c'est la classe d'une section hyperplane de la quadrique $X \subset \mathbb{P}^3_k$.
(e) Il y a une suite exacte naturelle

$$0 \to \mathrm{Pic}(X) \to \mathrm{Pic}(\overline{X})^g \to \mathrm{Br}(k) \to \mathrm{Br}_{alg}(X) \to 0.$$

(f) On a $X(k) \neq \emptyset$ si et seulement si $X(k(\sqrt{d})) \neq \emptyset$.

Soit $Y \subset \mathbb{A}^3_k$ une quadrique affine lisse définie par une équation $q(x, y, z) = a$, avec q forme quadratique non dégénérée et $a \in k^\times$.
Supposons $Y(k) \neq \emptyset$.
Montrer
(a) $\overline{k}^\times = \overline{k}[Y]^\times$, et $\mathrm{Pic}(Y) = \mathrm{Pic}(\overline{Y})^g$.
(b) Si $-a.det(q) \in k^{\times 2}$, alors $\mathbb{Z} = \mathrm{Pic}(Y) = \mathrm{Pic}(\overline{Y})^g$ et $\mathrm{Br}(k) = \mathrm{Br}_{alg}(Y)$
(c) Si $-a.det(q) \notin k^{\times 2}$, alors $0 = \mathrm{Pic}(Y) = \mathrm{Pic}(\overline{Y})^g$ et $\mathrm{Br}_{alg}(Y)/\mathrm{Br}(k) = \mathbb{Z}/2$.

Groupe de Brauer des schémas

Soit A un anneau de valuation discrète complet de corps des fractions K, de corps résiduel F parfait. On a des inclusions $K \subset K_{nr} \subset \overline{K}$ et $F \subset \overline{F}$. Ici K_{nr} est l'extension maximale non ramifiée. Le groupe de Galois G de K_{nr} sur K est le groupe de Galois de $\overline{F}$ sur F. En utilisant la flèche de valuation $K_{nr}^{\times} \to \mathbb{Z}$, on obtient une flèche

$$H^2(G, K_{nr}^{\times}) \to H^2(G, \mathbb{Z}) \simeq H^1(G_F, \mathbb{Q}/\mathbb{Z}).$$

On a une flèche naturelle $H^2(G, K_{nr}^{\times}) \to H^2(G_K, \overline{K}^{\times})$ dont on montre qu'elle est un isomorphisme. On obtient donc ainsi une flèche, dite "résidu"

$$\partial_A : \mathrm{Br}(K) \to H^1(F, \mathbb{Q}/\mathbb{Z}).$$

Ceci induit une flèche analogue

$$\partial_A : \mathrm{Br}(K) \to H^1(F, \mathbb{Q}/\mathbb{Z}).$$

pour tout anneau de valuation discrète A de corps résiduel F parfait.
Cette flèche associe à la classe d'une algèbre de quaternions $(a, b)_K$ (avec $a, b \in K^\times$) la classe de

$$(-1)^{v(a)v(b)} a^{v(b)} / b^{v(a)} \in A^\times$$

dans le quotient $F^\times / F^{\times 2} = H^1(F, \mathbb{Z}/2) \subset H^1(F, \mathbb{Q}/\mathbb{Z})$.

Pour X une variété lisse intègre sur un corps k de caractéristique zéro, on peut définir le groupe de Brauer non ramifié de X

$$\mathrm{Br}_{nr}(X) := \bigcap_{x \in X^{(1)}} Ker(\partial_x) \subset \mathrm{Br}(k(X)).$$

Cette définition élémentaire permet par exemple de voir que si X/k est projective et k-birationnelle à un espace projectif, alors $\mathrm{Br}(k) \simeq \mathrm{Br}_{nr}(X)$.
Mais elle ne permet pas de démontrer que le groupe est fonctoriel contravariant par morphisme quelconque de variétés lisses.
En particulier, on ne voit pas comment définir une évaluation sur les points rationnels

$$\mathrm{Br}_{nr}(X) \times X(k) \to \mathrm{Br}(k).$$

Pour définir le groupe de Brauer d'un schéma X quelconque, de façon fonctorielle en X, on peut
– soit utiliser une version terre à terre, en passant des algèbres simples centrales sur les corps aux algèbres d'Azumaya sur les schémas (comme on passe des vectoriels sur les corps aux fibrés vectoriels sur les schémas), ce qui donne un groupe $\mathrm{Br}_{Az}(X)$
– soit utiliser la cohomologie étale (Grothendieck), qui est une extension sur les schémas de la cohomologie galoisienne sur les corps, et définir $\mathrm{Br}(X) = H^2_{et}(X, \mathbb{G}_m)$.

On a pour tout schéma X une flèche injective $\mathrm{Br}_{Az}(X) \hookrightarrow \mathrm{Br}(X)$, qui pour X une k-variété algébrique quasiprojective lisse est un isomorphisme (Gabber).

On montre (SGA4) que pour une variété lisse intègre sur un corps k de car. zéro, on a $\mathrm{Br}(X) = \mathrm{Br}_{nr}(k(X)) \subset \mathrm{Br}(k(X))$, c'est-à-dire qu'on a une suite exacte

$$0 \to \mathrm{Br}(X) \to \mathrm{Br}(k(X)) \to \oplus_{x \in X^{(1)}} H^1(k(x), \mathbb{Q}/\mathbb{Z}).$$

Une conséquence est l'invariance k-birationnelle de $\mathrm{Br}(X)$ pour les k-variétés projectives lisses intègres.

Calculs de groupes de Brauer

On suppose maintenant $car(k) = 0$ et X k-variété lisse géométriquement intègre. On note $\overline{X} := X \times_k \overline{k}$.
L'étude du groupe de Brauer de X se décompose naturellement en deux parties.
Étude du groupe de Brauer de $\overline{X}$ et de l'image de $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})$ (appelée "groupe de Brauer transcendant").
Étude de

$$\mathrm{Br}_1(X) := Ker[\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})].$$

On peut montrer $\mathrm{Br}_1(X) = \mathrm{Br}_{alg}(X)$ comme défini plus haut.
On s'intéresse dans ces exposés principalement à des variétés pour lesquelles on sait déjà montrer $\mathrm{Br}(\overline{X}) = 0$.

Soit X/k lisse géométriquement intègre telle que $\overline{k}^\times = \overline{k}[X]^\times$. En utilisant la cohomologie étale, on établit une suite exacte

$$0 \to \operatorname{Pic} X \to (\operatorname{Pic} \overline{X})^{\operatorname{Gal}(\overline{k}/k)} \to^* \operatorname{Br} k \to$$

$$\operatorname{Br}_1 X \to \mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \to^* \mathrm{H}^3(k, \overline{k}^\times)$$

où les applications avec $*$ sont nulles si $X(k) \neq \emptyset$. Le groupe $\mathrm{H}^3(k, \overline{k}^\times)$ est trivial si k est un corps de nombres (théorie du corps de classes global).
Il y a des cas où il est facile de calculer $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ mais il est difficiel de relever explicitement les éléments de ce groupe dans $\operatorname{Br}_1(X)$.

Pour plus de détails sur le calcul du groupe de Brauer, je renvoie à mes notes de Bremen 2005, auxquelles j'ai ajouté quelques remarques.

Retour à l'arithmétique

Corps de nombres

Un corps de nombres k est un corps extension finie de $\mathbb{Q}$.
On note Ω l'ensemble des valeurs absolues ("places") , archimédiennes ou non, de k. Les complétions k_v sont dits "corps locaux".
Pour $v \in \Omega$ non archimédienne, i.e. v valuation discrète $v : k^* \to \mathbb{Z}$, la complétion k_v est une extension finie d'un corps $\mathbb{Q}_p$. On note $O_v \subset k_v$ l'anneau des entiers.
Pour $v \in \Omega$ archimédienne, la complétion k_v est soit $\mathbb{R}$ soit $\mathbb{C}$. On note $O_v = k_v$.
Pour $S \subset \Omega$ un ensemble fini de places contenant les places archimédiennes, on note $O_S \subset k$ l'anneau des S-entiers ($v(x) \geq 0$ pour $v \notin S$).

Approximation faible
Pour tout ensemble fini $S \subset \Omega$, l'image diagonale de $k \to \prod_{v \in S} k_v$ est dense.

Approximation forte
Soient $S \subset \Omega$ un ensemble fini de places contenant les places archimédiennes. Pour $v \in S$, soit $U_v \subset k_v$ un ouvert non vide. Soit $v_0 \in S$. L'ensemble

$$\prod_{v \in S \setminus \{v_0\}} U_v \times \prod_{v \notin S} O_v$$

contient l'image diagonale d'un élément de k.
En d'autres termes k est dense dans le "produit restreint", pour $v \neq v_0$, des k_v par rapport aux O_v.
Ceci est une généralisation du théorème du reste chinois.

Pour un corps local k_v, il existe un plongement naturel

$$i_v : \mathrm{Br}(k_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

On a $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2$ engendré par la classe des quaternions de Hamilton et $\mathrm{Br}(\mathbb{C}) = 0$.
Pour v une place finie, i_v est un isomorphisme donné par l'application résidu

$$\partial_v : \mathrm{Br}(k_v) \to H^1(F_v, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$$

décrite plus haut. Le signe est déterminé par le choix du générateur du groupe de Galois absolu des corps finis.
On a de fait $\mathrm{Br}(O_v) = \mathrm{Br}(F_v) = 0$,
où O_v est l'anneau des entiers de k_v et F_v le corps fini résiduel.

Un théorème fondamental de la *théorie du corps de classes* est que ces applications i_v donnent naissance à une suite exacte

$$0 \to \mathrm{Br}(k) \to \bigoplus_v \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

– Cet énoncé implique le principe de Hasse pour $Norm_{K/k}(x) = c$ si K/k est cyclique.
– Le fait que le composé soit zéro contient la loi de réciprocité quadratique et ses compléments. C'est une traduction dans le cas de la classe $(p, q) \in \mathrm{Br}(\mathbb{Q})$ d'une algèbre de quaternions, avec p et q premiers.
– La suite exacte aussi contient le fait que si une conique sur un corps de nombres a des points dans tous les complétés k_v sauf peut-être un, k_{v_0}, alors elle en possède un dans k_{v_0} et dans k.

Variétés sur un corps de nombres, principe de Hasse, approximation faible, approximation forte

Soit X une k-variété lisse géométriquement intègre sur un corps de nombres k.
On dit que l'**approximation faible** vaut pour X si l'image diagonale

$$X(k) \to \prod_{v \in \Omega} X(k_v)$$

est dense, la topologie à droite étant la topologie produit.
Cette définition de l'approximation faible contient le principe de Hasse pour les points rationnels.
Cette notion est k-birationnelle. On peut ainsi se limiter à la considérer des variétés projectives.

Cas classiques

– Espace projectif $\mathbb{P}^n_k$
– Quadriques lisses (Hasse)
– Variétés de Severi-Brauer (F. Châtelet)
– Équation $Norm_{K/k}(x) = c$ pour K/k cyclique (Hasse)
– Espace principal homogène de groupe algébrique semisimple simplement connexe (Eichler, Kneser, Harder, Chernousov)
– Variétés projectives espaces homogènes de groupe algébrique linéaire connexe (Harder) : ceci couvre le cas des quadriques et des variétés de Severi-Brauer
– Espace principal homogène de k-tore k-rationnel (Voskresenskiĭ)

Cas conjecturé
Système d'équations

$$y_i^2 - a_i z_i^2 = P_i(x) \neq 0, \quad i = 1, \ldots, n$$

avec $a_i \in k^\times$ et les polynômes $P_i(x)$ irréductibles.

Connu pour $y^2 - az^2 = P(x)$ avec $P(x)$ irréductible de degré 4 (CT, Sansuc, Swinnerton-Dyer 1987).

Connu en général modulo l'hypothèse BDS (hypothèse de Bouniakowsky-Dickson-Schinzel : hypothèse des nombres premiers jumeaux généralisée).

Cas conjecturés

– Hypersurface cubique lisse dans $\mathbb{P}^n_k$ pour $n \geq 4$. Connu pour $n \geq 9$ (Heath-Brown sur $\mathbb{Q}$, très récent résultat de Browning-Vishe sur un corps de nombres)

– Intersection complète lisse de deux quadriques dans $\mathbb{P}^n_k$ pour $n \geq 5$.

Connu pour $n \geq 8$ (CT, Sansuc, Swinnerton-Dyer 1987).

Résultat conditionnel (modulo BDS et Tate-Shafarevich) pour $n \geq 5$: Wittenberg.

Soit X une k-variété lisse géométriquement intègre sur un corps de nombres k. Soit $S \subset \Omega$ un ensemble fini *non vide*. On dit que **l'approximation forte en dehors de** S vaut pour X si on a la propriété suivante.
Pour tout ensemble fini T de places contenant S et les places archimédiennes et toute famille d'ouverts non vides $U_v \subset X(k_v)$ pour $v \in T \setminus S$, et tout O_T-schéma de type fini $\mathcal{X}/O_T$ modèle de X/k, i.e. $\mathcal{X} \times_{O_T} k \simeq X$, si le produit

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

est non vide, alors il existe un point de $X(k)$, donc de $\mathcal{X}(O_T)$, dans ce produit.

Un tel énoncé contient un principe local-global pour l'existence de O_S-points entiers sur les O_S-modèles de X :

Pour $\mathcal{X}/O_S$ un modèle entier de X/k, si l'on a

$$\prod_{v \in S \cup \infty} X(k_v) \times \prod_{v \notin S \cup \infty} \mathcal{X}(O_v) \neq \emptyset,$$

alors $\mathcal{X}(O_S) \neq \emptyset$.

Soit $X(\mathbb{A}_k)$ l'espace des adèles de X, supposé non vide, et soit $X(\mathbb{A}_k^S)$ l'espace des adèles hors de S. Ces espaces sont équipées d'une topologie qui diffère de la topologie produit si X/k n'est pas projective.
L'approximation forte hors de S vaut si et seulement si l'image diagonale de $X(k)$ dans $X(\mathbb{A}_k^S)$ est dense pour la topologie adélique.
[Pour une variété projective X/k, il y a approximation forte hors de tout S fini si et seulement si il y a approximation faible.]

Exemple de base : le groupe additif $\mathbb{G}_a$ sur le corps k.

Théorème (Eichler, Kneser, Platonov) Soit G un k-groupe semisimple simplement connexe absolument presque simple. Soit v une place. Si le groupe $G(k_v)$ est non compact, alors l'approximation forte hors de v vaut pour G.
Exemple : $G = SL(D)$ pour D une algèbre simple centrale avec une place $v \in S$ telle que $D \otimes_k k_v$ n'est pas un corps gauche.

Théorème (Eichler, Kneser) Soit q une forme quadratique non dégénérée en $n \geq 4$ variables sur k, supposons que q est isotrope sur k_v. Alors pour tout $a \in k^\times$ l'approximation forte hors de $\{v\}$ vaut pour

$$q(x_1, \ldots, x_n) = a.$$

Ensemble de Brauer-Manin

Grâce à la fonctorialité du groupe de Brauer, on a pour tout anneau commutatif R et tout R-schéma X un accouplement

$$X(R) \times \mathrm{Br}(X) \to \mathrm{Br}(R).$$

On établit les fait suivants.

Proposition. *Pour X une variété sur un corps local et $A \in \mathrm{Br}(X)$ l'évaluation*

$$ev_A : X(k) \to \mathrm{Br}(k) \subset \mathbb{Q}/\mathbb{Z}$$

est localement constante sur $X(k)$ pour la topologie naturelle induite par celle de k.

Proposition. *Soit k un corps local non archimédien et $O \subset k$ son anneau d'entiers. Pour $\mathcal{X}$ un schéma sur un anneau local $O_v \subset k_v$ et $A \in \mathrm{Br}(\mathcal{X})$ l'application d'évaluation*

$$ev_A : \mathcal{X}(O) \to \mathrm{Br}(k) \subset \mathbb{Q}/\mathbb{Z}$$

est nulle.

Proposition. *Pour X une variété projective sur un corps de nombres et $A \in \mathrm{Br}(X)$, pour presque toute place v, l'évaluation $ev_A : X(k_v) \to \mathrm{Br}(k_v)$ est nulle.*

Plus généralement :

Proposition. *Soit k un corps de nombres, O son anneau des entiers, S un ensemble fini de places contenant les places archimédiennes, O_S l'anneau des S-entiers. Soit $\mathcal{X}$ un schéma intègre de type fini sur O_S et soit $X = \mathcal{X} \times_{O_S} k$. Soit $A \in \mathrm{Br}(X)$. Pour presque toute place v de k, pour tout $P_v \in \mathcal{X}(O_v)$, on a $A(P_v) = 0$.*

Cette proposition admet une sorte de réciproque.

Proposition (Harari) *Soit 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 $\alpha(M_v) \neq 0$.*

Le cas le plus simple est le suivant. On considère $a \in k^*$, a non carré dans k, on prend $X = \mathbb{A}^1_k = Spec(k[t])$, 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 $(a, t_v) \neq 0 \in \mathrm{Br}(k_v)$.

Par un argument essentiellement combinatoire, on établit alors l'énoncé fort utile suivant.

Proposition (Harari, "Lemme formel") *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 $\{P_v\} \in U(\mathbb{A}_k)$. 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 $\{M_v\} \in U(\mathbb{A}_k)$ telle que $M_v = P_v$ pour $v \in S$ et tel que pour tout $\beta \in B$ on ait

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

Soit X une k-variété lisse intègre. Les propositions (directes) ci-dessus montrent que pour tout $A \in \mathrm{Br}(X)$ l'application

$$\theta_A : X(\mathbb{A}_k) \to \mathbb{Q}/\mathbb{Z}$$

définie par

$$\{P_v\} \to \sum_{v \in \Omega} i_v(A(P_v))$$

est bien définie (pour tout adèle, c'est une somme finie, et que son noyau $Ker(\theta_A)$ (les points d'image nulle) est ouvert et fermé dans $X(\mathbb{A}_k)$.

On définit alors

$$X(\mathbb{A}_k)^{Br} =: \bigcap_{A \in \mathrm{Br}(X)} Ker(\theta_A).$$

C'est l'ensemble de Brauer-Manin de X. Il est fermé dans $X(\mathbb{A}_k)$. D'après la loi de réciprocité généralisée, on a

$$X(k) \subset X(\mathbb{A}_k)^{Br} \subset X(\mathbb{A}_k).$$

L'adhérence de $X(k)$ dans $X(\mathbb{A}_k)$ (pour la topologie adélique) est dans $X(\mathbb{A}_k)^{Br}$.

Points rationnels : Obstruction de Brauer-Manin, principe de Hasse et approximation faible

L'exemple de Lind du point de vue de l'obstruction de Brauer-Manin

L'équation

$$2y^2 = x^4 - 17 \neq 0$$

définit un ouvert U d'une courbe projective lisse $X/\mathbb{Q}$.

On a $\prod_{p \cup \infty} X(\mathbb{Q}_p) \neq \emptyset$.

Exercice : L'algèbre de quaternions $(y, 17) \in \mathrm{Br}(U)$ est la restriction d'une classe $A \in \mathrm{Br}(X)$.

Pour $p \neq 17$ l'image de $ev_A : X(\mathbb{Q}_p) \to \mathrm{Br}(\mathbb{Q}_p) \subset \mathbb{Q}/\mathbb{Z}$ est nulle si $p \neq 17$.

Pour $p = 17$ l'image de $ev_A : X(\mathbb{Q}_{17}) \to \mathrm{Br}(\mathbb{Q}_{17}) \subset \mathbb{Q}/\mathbb{Z}$ est $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$.

Donc $X(\mathbb{Q}) = \emptyset$.

L'exemple d'Iskovskikh du point de vue de l'obstruction de Brauer-Manin

Soit $c \in \mathbb{Z}, c > 0, c$ impair. L'équation

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

définit un ouvert U_c dans une surface projective lisse $X_c/\mathbb{Q}$.
On a $\prod_{p \cup \infty} X_c(\mathbb{Q}_p) \neq \emptyset$.
L'algèbre de quaternions $(c - x^2, -1) \in \mathrm{Br}(U_c)$ s'étend en $A \in \mathrm{Br}(X_c)$.

$$y^2 + z^2 = (c - x^2)(x^2 - c + 1) \neq 0$$

Pour $p \neq 2$, l'image de

$$ev_A : X_c(\mathbb{Q}_p) \to \mathrm{Br}(\mathbb{Q}_p) \subset \mathbb{Q}/\mathbb{Z}$$

est nulle.
Pour $p = 2$, cette image est $\{1/2\} \subset \mathbb{Q}/\mathbb{Z}$ si et seulement si $c \equiv 3(4)$.
Ainsi : *Si* $c \equiv 3(4)$, *alors* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}(X)} = \emptyset$, *et donc* $X_c(\mathbb{Q}) = \emptyset$.
Le même calcul montre : *Si* $c \equiv 1(4)$, *alors* $X_c(A_{\mathbb{Q}})^{\mathrm{Br}(X)} \neq \emptyset$.

Théorème *Si* $c \equiv 1(4)$ *alors* $X_c(\mathbb{Q}) \neq \emptyset$.
(cas particulier d'un théorème de CT, Coray et Sansuc, 1981)

Soit X une k-variété lisse, géométriquement intègre, *projective*.
On dit que l'approximation faible avec condition de Brauer-Manin vaut pour X si l'adhérence de $X(k)$ dans $X(\mathbb{A}_k)$ coïncide avec $X(\mathbb{A}_k)^{Br}$.
Un tel énoncé contient la propriété suivante : si $X(\mathbb{A}_k)^{Br} \neq \emptyset$, alors $X(k) \neq \emptyset$: l'obstruction de Brauer-Manin au principe de Hasse pour les points rationnels est la seule obstruction à l'existence d'un point rationnel.

Théorème (Sansuc, Borovoi) Soit X une k-variété projective et lisse intègre qui contient un ouvert U espace homogène d'un k-groupe algébrique linéaire, les stabilisateurs géométriques étant connexes. Alors $X(k)$ est dense dans $X(\mathbb{A}_k)^{Br}$.

Les démonstrations utilisent :

Le principe de Hasse pour les espaces principaux homogènes de groupes semisimples simplement connexes (Kneser, Harder, Chernousov)

La théorie du corps de classes : la dualité de Tate-Nakayama pour les tores.

Conjecture (CT-Sansuc) Soit k un corps de nombres. Pour X une k-surface projective, lisse, (géométriquement) rationnelle, $X(k)$ est dense dans $X(\mathbb{A}_k)^{Br}$. En particulier, si $\mathrm{Br}(X)/\mathrm{Br}(k) = 0$, le principe de Hasse et l'approximation faible valent.

La conjecture est connue pour $y^2 - az^2 = P(x)$ avec $P(x)$ de degré 3 ou 4 (CT-Sansuc-Swinnerton-Dyer).

Il y a essentiellement deux familles de telles surfaces rationnelles : les surfaces fibrées en coniques au-dessus d'une conique, et les surfaces de del Pezzo, parmi lesquelles les surfaces cubiques lisses.

De nombreux tests numériques ont été faits sur les surfaces cubiques

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

avec $a, b, c, d \in \mathbb{Z}$, sans facteur cubique.
Si une telle surface $X/\mathbb{Q}$ a des points dans tous les $\mathbb{Q}_p$, et s'il existe un nombre premier p qui ne divise qu'un seul des a, b, c, d, alors $X(\mathbb{A}_{\mathbb{Q}})^{Br} \neq \emptyset$ (CT-Kanevsky-Sansuc 1987).

La conjecture BDS implique la conjecture de CT-Sansuc sur les points rationnels pour les surfaces rationnelles fibrées en coniques.

Une version zéro-cycles de la conjecture a été établie pour les surfaces fibrées en coniques par Salberger.

Exemple 1. Soient $P(x) = P_1(x).P_2(x)$ le produit de deux polynômes irréductibles de degrés *pairs* premiers entre eux et $a \in k^\times$. Soit Y la surface lisse d'équation $y^2 - az^2 = P(x)$ et soit X une k-compactification lisse de Y. Montrer que l'algèbre de quaternions $A = (a, P_1(x))$ est dans $\mathrm{Br}(X)$, et engendre $\mathrm{Br}(X)/\mathrm{Br}(k)$. S'il n'y a pas d'obstruction de Brauer-Manin pour X, alors il existe $c \in k^\times$ tel que le système d'équations

$$y_1^2 - az_1^2 = c.P_1(x), \;\; y_2^2 - az_2^2 = c^{-1}.P_1(x)$$

admette des solutions dans tous les k_v.
L'hypothèse que P_1 et P_2 sont irréductibles et la conjecture BDS impliquent l'existence d'une solution de ce sytème dans k. Une telle solution en donne une pour $y^2 - az^2 = P(x)$.

Exemple 2. Soient $P(x) = P_1(x).P_2(x)$ le produit de deux polynômes irréductibles de degrés *impairs* premiers entre eux et $a \in k^\times$. Si la surface Y d'équation $y^2 - az^2 = P(x)$ a des points dans tous les k_v, alors il existe $c \in k^\times$ tel que le système d'équations

$$y_1^2 - az_1^2 = c.P_1(x), \;\; y_2^2 - az_2^2 = c^{-1}.P_1(x)$$

admette des solutions dans tous les k_v. Pour établir ce résultat, on utilise un cas particulier du lemme formel.
L'hypothèse que P_1 et P_2 sont irréductibles et la conjecture BDS impliquent l'existence d'une solution de ce sytème dans k. Une telle solution en donne une pour $y^2 - az^2 = P(x)$.
Montrer que pour X un modèle projectif et lisse de la surface Y, on a $\mathrm{Br}(X)/\mathrm{Br}(k) = 0$. L'algèbre de quaternions $(a, P_1(x) \in \mathrm{Br}(k(X))$ est ramifiée, elle n'est pas dans $\mathrm{Br}(X)$.

Il existe des variétés X/k projectives lisses géométriquement intègres avec $X(\mathbb{A}_k)^{Br} \neq \emptyset$ et $X(k) = \emptyset$.
Skorobogatov (1999); Poonen (2009).
De nouvelles obstructions ont été définies (Harari, Skorobogatov), qui rendent compte de l'exemple de Skorobogatov.
Mais ces obstructions ne rendent pas compte des exemples (simples) de Poonen.
Il y a des travaux en cours impliquant l'homotopie étale qui essayent de définir des obstructions "supérieures".

Méthodes de fibration

Soit $f : X \to \mathbb{P}^1_k$ un morphisme dominant. Si l'on contrôle le principe de Hasse dans les fibres, au moins au moyen de l'obstruction de Brauer-Manin, peut-on le contrôler pour l'espace total X ?
En utilisant de façon cruciale son "Lemme formel", Harari a établi l'énoncé suivant.

Théorème (D. Harari 1994)
Soit $f : X \to \mathbb{P}^1_k$ comme ci-dessus. On suppose X projective, lisse, géométriquement intègre. Soit $K = k(\mathbb{P}^1)$. On suppose :
La fibre générique géométrique $X_\eta \times_K \overline{K}$ a son groupe de Picard libre de type fini et son groupe de Brauer nul.
Toutes les fibres aux points fermés de $\mathbb{A}^1$ ont une composante géométriquement intègre de multiplicité 1.
La fibration $X \to \mathbb{P}^1$ admet une section sur $\overline{k}$.
L'obstruction de Brauer-Manin au principe de Hasse est la seule obstruction pour les fibres X_t/k pour presque tout $t \in \mathbb{P}^1(k)$ (en fait un ensemble de Hilbert suffit).
Alors l'obstruction de Brauer-Manin au principe de Hasse est la seule pour l'espace total X.

Combiné avec un résultat antérieur de Salberger et Skorobogatov sur les surfaces cubiques contenant une droite k-rationnelle, ce théorème permet d'établir l'approximation faible pour toute hypersurface cubique lisse dans $\mathbb{P}^4_k$, lorsque cette hypersurface contient une droite k-rationnelle : on fibre l'hypersurface avec les $\mathbb{P}^3$ contenant la droite donnée.

Ce théorème montre aussi que si la conjecture sur l'obstruction de Brauer-Manin pour les surfaces cubiques est vraie, alors le principe de Hasse et l'approximation faible valent pour les hypersurfaces cubiques lisses dans $\mathbb{P}^n_k$ pour $n \geq 4$. Le groupe de Brauer de telles hypersurfaces est en effet réduit à $\mathrm{Br}(k)$.

Points entiers : Obstruction de Brauer-Manin, principe de Hasse et approximation forte

Soit X une k-variété lisse géométriquement intègre sur un corps de nombres k. Soit $S \subset \Omega$ un ensemble fini *non vide*. On dit que l'**approximation forte hors de S avec condition de Brauer-Manin** vaut pour X si on a la propriété suivante.

Pour tout ensemble fini T de places contenant S et les places archimédiennes et toute famille d'ouverts non vides $U_v \subset X(k_v)$ pour $v \in T \setminus S$, et tout O_T-schéma de type fini $\mathcal{X}/O_T$ modèle de X/k, i.e. $\mathcal{X} \times_{O_T} k \simeq X$, si l'ensemble

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

est non vide, alors il existe un point de $X(k)$, donc de $\mathcal{X}(O_T)$, dans cet ensemble.

Sorites

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

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

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

[Utilise le lemme formel d'Harari.]

Dans les contre-exemples à l'approximation forte donnés tout au début, on a $k = \mathbb{Q}$, $S = \infty$, $\mathcal{X}$ over $\mathbb{Z}$, et on peut montrer :

$$[X(\mathbb{R}) \times \prod_{p \neq \infty} \mathcal{X}(\mathbb{Z}_p)]^{\mathrm{Br}X} = \emptyset,$$

donc (par réciprocité) $\mathcal{X}(\mathbb{Z}) = \emptyset$.

Dans l'exemple de Borovoi–Rudnick $\mathcal{X}/\mathbb{Z}$

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

on utilise la classe de l'algèbre de quaternions
$(y-x,2) = (9x+7y,2) \in \mathrm{Br}(X)$.

Dans l'exemple trivial $\{2x-5y=1, xt=1\}$ sur $\mathbb{Q}$, on peut utiliser l'algèbre de quaternions $(x,5)$. L'argument montre alors que l'équation n'a pas de solution entière dans une extension $K/\mathbb{Q}$ de degré impair non ramifiée et totalement scindée en 2 et 5.

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

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

CT et Xu 2005-2009 (G semisimple simplement connexe); Harari 2008 (G commutatif connexe); Demarche 2011 (groupes quelconques); Borovoi et Demarche (espaces homogènes, cas général).
Pour G semisimple simplement connexe, $\mathrm{Br}(X)/\mathrm{Br}(k)$ est fini. Ce n'est pas le cas pour G un k-tore, par exemple $\mathrm{Br}(X)/\mathrm{Br}(k)$ est infini pour X donné par $x^2 - ay^2 = b$.

Les démonstrations utilisent :

Le principe de Hasse pour les espaces principaux homogènes de groupes semisimples simplement connexes (Kneser, Harder, Chernousov)

La théorie du corps de classes : la dualité de Tate-Nakayama pour les tores, une généralisation non commutative (Kottwiz), et des extensions à des théorèmes de dualité pour les complexes de tores (Demarche)

L'approximation forte hors de S pour les groupes semisimples avec une condition de non compacité.

Le cas intéressant le plus simple

Soit Y la k-variété définie par $q(x,y,z) = c$, avec q forme quadratique ternaire non dégénérée et $c \in k^\times$. Supposons $Y(k) \neq \emptyset$.

C'est un espace homogène sous le groupe des spineurs de q, les stabilisateurs sont des tores de dimension 1.

Soit $d = -c.\det(q)$.

Si $d \in k^{\times 2}$ alors $\mathrm{Br}(Y)/\mathrm{Br}(k) = 0$.

Si $d \notin k^{\times 2}$ alors $\mathrm{Br}(Y)/\mathrm{Br}(k) = \mathbb{Z}/2$, engendré par un élément $\xi \in \mathrm{Br}(Y)$ d'ordre 2, de la forme $(l(x,y,z), d)$ avec $l(x,y,z)$ fonction linéaire affine convenable (définissant l'espace tangent en un k-point).

Sur k corps de nombres, pour S fini contenant une place v avec q isotrope en v, on a l'approximation forte hors de S avec condition de Brauer-Manin – qui se réduit à la condition définie par ξ.

Calculs

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

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

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

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

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

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

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

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

On va utiliser une méthode de fibrations pour étudier les points entiers de ces variétés.

Théorème (CT et Fei XU, 2011)

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

$k = \mathbb{Q}$, S la place réelle.

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

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

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

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

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

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

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

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

Expliquons la démonstration du dernier théorème dans un cas particulier.

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

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

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

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

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

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

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

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

Supposons maintenant $P(t) = c.(r(t))^2$, soit $P(t) = c.\prod_i P_i(t)^{e_i}$, avec les $P_i \in k[t]$ irréductibles et les e_i tous pairs.
Soit $d = -c.det(q)$. Soit $k_i = k[t]/(P_i)$.
Exercice.
• Si d carré dans k, alors $\mathrm{Br}(\tilde{X})/\mathrm{Br}(k) = \mathrm{Br}(U)/\mathrm{Br}(k) = 0$.
• Si d non carré dans k et il existe un i avec d non carré dans k_i, alors $\mathrm{Br}(\tilde{X})/\mathrm{Br}(k) = 0$ et $\mathrm{Br}(U)/\mathrm{Br}(k) = \mathbb{Z}/2$.
• Si d non carré dans k et carré dans chaque k_i, alors $\mathrm{Br}(\tilde{X})/\mathrm{Br}(k) = \mathrm{Br}(U)/\mathrm{Br}(k) = \mathbb{Z}/2$.
• De plus, pour tout $t_0 \in k$ avec $p(t_0) \neq 0$, la spécialisation $\mathrm{Br}(U)/\mathrm{Br}(k) \to \mathrm{Br}(U_{t_0})/\mathrm{Br}(k)$ est surjective.

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

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

où U_v est un ouvert dans $U(k_v)$:

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

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

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

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

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

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

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

Les résultats ci-dessus admettent des généralisations aux fibrations en espaces homogènes de groupes semisimples (CT-Harari, 2012). Je me contenterai de citer le résultat suivant.

Théorème *Soit X l'ouvert de lissité de la k-variété affine Y d'équation*

$$\sum_{i=0}^{2} a_i(t)x_i^2 = p(t),$$

où les $a_i(t)$ et $p(t)$ dans $k[t]$ sont des polynômes deux à deux premiers entre eux. Soit v_0 une place de k.
(i) Si la conique d'équation $\sum_{i=0}^{2} a_i(t)x_i^2 = 0$ sur le corps $k(t)$ a un point rationnel sur le corps $k_{v_0}(t)$, alors l'approximation forte hors de v_0 avec condition de Brauer-Manin vaut pour X.
(ii) Si de plus les produits $p(t).\prod_i a_i(t)$, est un polynôme séparable, alors $X = Y$ et l'approximation forte vaut pour X hors de v_0 : l'image diagonale de $X(k)$ est dense dans $X(\mathbb{A}_k^{v_0})$.

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

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

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