Introduction au domaine de recherche

Giancarlo Lucchini Servetto

Sous la direction de David Harari

École Normale Supérieure

Juin 2011

Cohomologie galoisienne et arithmétique des groupes algébriques

Table des matières

Introduction **3**

1 Les frères de $\mathbb{R}$, les corps $\mathbb{Q}_p$ **3**
1.1 La valeur absolue p-adique 3
1.2 Définition et propriétés de $\mathbb{Q}_p$ 4
1.3 Théorème d'Ostrowski 5
1.4 Le principe de Hasse 6

2 Cohomologie **7**
2.1 Rappels de cohomologie des groupes 7
2.2 Cohomologie galoisienne 8
2.3 Cohomologie étale 9
2.4 L'obstruction de Brauer-Manin 10
2.5 Un mot sur la cohomologie non abélienne 11

3 Espaces homogènes **12**
3.1 Définition et propriétés 12
3.2 Quelques résultats récents et questions à résoudre 13

Références **15**

Introduction

C'est en 1900 que David Hilbert donna sa célèbre liste de 23 problèmes à résoudre par les mathématiciens du XX$^{\text{ème}}$ siècle. Le problème numéro 10 proposait notamment de trouver un algorithme permettant de savoir si une équation diophantienne (i.e. polynomiale à coefficients entiers) a ou non des solutions sur $\mathbb{Z}$. Ce qu'il faut comprendre ici comme *algorithme* est l'existence d'un "test" que l'on puisse programmer sur un ordinateur (une machine de Turing devrait suffire) et qui s'arrête en temps fini pour dire si un polynôme donné a des solutions ou non. Matiiassevich a démontré en 1970 qu'un tel algorithme ne peut exister. Mais on peut alors être un peu moins gourmand et se demander s'il existe un tel algorithme pour des solutions sur $\mathbb{Q}$. Ce problème reste encore ouvert aujourd'hui.
Une façon de résoudre ce problème serait de donner une quantité finie de paramètres à calculer pour chaque équation, avec lesquelles on puisse décider si elle a des solutions sur $\mathbb{Q}$ ou non. Une condition nécessaire et facile à calculer est qu'elle ait des solutions sur $\mathbb{R}$. Cette idée à l'air naïve est en fait à la base d'un principe qui a donné pour un certain temps de l'espoir pour une réponse positive à cette question : c'est le *principe de Hasse*, qui est le sujet de cet exposé.

1 Les frères de $\mathbb{R}$, les corps $\mathbb{Q}_p$

C'est clair, le critère d'avoir ou non des solutions sur $\mathbb{R}$ n'est pas suffisant. Mais ce qui fait que ce critère soit déjà non trivial, est le fait que $\mathbb{R}$ est un corps contenant $\mathbb{Q}$, qui n'est pas algébriquement clos (sur $\mathbb{C}$ par exemple il y a toujours des solutions) et qui a une métrique induite par une valeur absolue par rapport à laquelle il est *complet*, ce qui nous permet d'utiliser des outils issus de l'analyse pour trouver des solutions aux équations.
Or, il se trouve que $\mathbb{R}$ n'est pas le seul corps vérifiant ces propriétés. En effet, il y a au moins un autre corps de ce type pour chaque nombre premier p. Ce sont ces corps que l'on va présenter maintenant. Pour plus de détails, on pourra regarder [LSW09] ou s'adresser aux livres de Gouvea [Gou00] et Robert [Rob00].

1.1 La valeur absolue p-adique

Fixons désormais un nombre premier p.

Pour construire les corps dits p-adiques, il faut changer notre notion de distance, on parlera alors de distance p-adique. En nous concentrant d'abord sur $\mathbb{Z}$, on dira que deux entiers relatifs sont "proches" l'un de l'autre s'ils sont congrus modulo p^n pour n très grand. Ainsi, on peut dire que p est plus proche de 0 que 1, et que p^2 l'est encore plus que p. En particulier, la puissance n-ième de p est plus "petite" lorsque n est plus grand. On dira que la distance entre deux nombres est plus petite que p^{-n} s'ils sont congrus modulo p^n. Notons que tout ceci a un sens aussi pour des puissances négatives de n. En effet, $\frac{1}{p}$ est plus proche de $\frac{p+1}{p}$ que de 1, car ils sont congrus modulo $\frac{1}{p}$, i.e. ils sont égaux lorsqu'on les regarde comme des éléments de $\mathbb{Q}/p^{-1}\mathbb{Q}$, alors que $\frac{1}{p}$ et 1 ne sont congrus modulo p^n que lorsque $n \leq -2$.
Ces idées admettent une définition formelle :

Définition 1.1. La *valuation p-adique* sur $\mathbb{Q}$ est la fonction $v_p : \mathbb{Q} \to \mathbb{Z} \bigcup \{+\infty\}$ qui a x associe le plus grand $n \in \mathbb{Z} \cup \{\infty\}$ tel que $x \equiv 0 \mod p^n$. En d'autres mots, $v_p(x)$ est le seul entier relatif n tel que $x = p^n \frac{a}{b}$ avec $a, b \in \mathbb{Z}$ et $\text{pgcd}(p, a) = \text{pgcd}(p, b) = 1$.
La *valeur absolue p-adique* est la fonction $|\cdot|_p : \mathbb{Q} \to \mathbb{Z}$ définie par la formule

$$|x|_p = p^{-v_p(x)}.$$

On notera que pour $x = 0$ la valuation p-adique est $+\infty$ et alors sa valeur absolue est 0, précisément comme on s'y attendrait. Comme on l'a dit plus haut, pour cette valeur absolue, les nombres qui sont "petits" sont ceux qui sont "très congrus" à 0 modulo p.

Remarque 1.2. La valuation p-adique vérifie les deux propriétés suivantes :

(i) $v_p(xy) = v_p(x) + v_p(y) \quad \forall x, y \in \mathbb{Q}$;

(ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\} \quad \forall x, y \in \mathbb{Q}$.

Ceci nous dit que la valeur absolue p-adique est bien une valeur absolue au sens classique : elle est multiplicative grâce à la propriété (i) et elle vérifie l'inégalité triangulaire grâce à la propriété (ii).

1.2 Définition et propriétés de $\mathbb{Q}_p$

De la même façon que l'on complète $\mathbb{Q}$ par rapport à la valeur absolue classique pour obtenir $\mathbb{R}$, on peut le compléter par rapport à une valeur absolue p-adique. Ce procédé consiste à considérer des classes d'équivalence des suites de Cauchy sur $\mathbb{Q}$ par rapport à la distance induite par $|\cdot|_p$. En gros, le complété serait le corps composé de toutes les limites de ces suites. Tous les détails sont dans [LSW09, Section 1.3].

Définition 1.3. On note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ par rapport à la valeur absolue $|\cdot|_p$ et on l'appelle le *corps des nombres p-adiques*. La valuation et la valeur absolue p-adique s'étendent à cette complétion naturellement. L'adhérence de $\mathbb{Z}$ dans ce corps est notée $\mathbb{Z}_p$ et est appelée l'*anneau des entiers p-adiques*.

Proposition 1.4. *Une suite $(a_i)_{i\in\mathbb{N}}$ est de Cauchy pour la distance p-adique si et seulement si pour tout $n \in \mathbb{N}$ il existe $N \in \mathbb{N}$ tel que pour tout $i, j \geq N$ on a $v_p(a_i - a_j) \geq n$.*

Démonstration. C'est en effet la définition d'une suite de Cauchy après avoir noté que la distance p-adique décroit vers 0 lorsque la valuation se rapproche de ∞. [$\breve{\smile}$]

Ceci nous dit qu'en particulier, pour $(b_k) \in \{0, 1, 2, \ldots, p-1\}^{\mathbb{N}}$, la suite

$$a_n = \sum_{k=0}^{n} b_k p^k,$$

est une suite de Cauchy, et alors sa limite fait partie du complété de $\mathbb{Q}$ par rapport à la valeur absolue p-adique. Plus précisément, on a la proposition suivante.

Proposition 1.5. *On a*

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{n} b_k p^k, (b_k) \in \{0, 1, 2, \ldots, p-1\}^{\mathbb{N}} \right\} = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

De plus, l'ensemble

$$\mathcal{P} = \left\{ \sum_{k=1}^{n} b_k p^k, (b_k) \in \{0, 1, 2, \ldots, p-1\}^{\mathbb{N}^*} \right\} = \{x \in \mathbb{Q}_p : v_p(x) > 0\} = \{x \in \mathbb{Q}_p : |x|_p < 1\}$$

est le seul idéal maximal de $\mathbb{Z}_p$. En fait, si $\pi \in \mathcal{P}$ vérifie $v(\pi) = 1$ (notamment, si $\pi = p$), alors tout idéal non nul de $\mathbb{Z}_p$ est de la forme $\mathcal{P}^n = \pi^n \mathbb{Z}_p$ avec $n \geq 1$.
En particulier, tout élément de $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ est inversible dans $\mathbb{Z}_p$.

Corollaire 1.6. *On a*

$$\mathbb{Q}_p = \left\{ \sum_{k=k_0}^{\infty} b_k p^k, k_0 \in \mathbb{Z}, b_k \in \{0, 1, 2, \ldots, p-1\} \ \forall k \geq k_0 \right\}.$$

Démonstration de la proposition. Il est facile de voir que toute suite de Cauchy sur $\mathbb{Z}$ peut s'écrire sous forme de suite de sommes partielles (il suffit de regarder les sommes des différences des termes consécutifs), ce qui donne les premières égalités. On vérifie aisément que tout élement dans $\mathbb{Z}_p \setminus \mathcal{P}$ est inversible dans $\mathbb{Z}_p$: si $v_p(x) = 0$, alors $v_p(x^{-1}) = -v_p(x) = 0$ et donc $x^{-1} \in \mathbb{Z}_p$.

Soit I un idéal non nul de $\mathbb{Z}_p$, en considérant l'ensemble $\{v_p(x) : x \in I\}$, on choisit $a \in I$ avec $n = v_p(a)$ minimal. On affirme que $I = a\mathbb{Z}_p = \pi^n(a\pi^{-n})\mathbb{Z}_p = \pi^n\mathbb{Z}_p$ (notons que $v(a\pi^{-n}) = 0$). Soit $x \in I$, alors $v_p(x) \geq v_p(a)$ donc $v_p(xa^{-1}) \geq 0$ et $xa^{-1} \in \mathbb{Z}_p$, i.e. $x \in a\mathbb{Z}_p$. [$\ddot\smile$]

Définition 1.7. Le corps $\mathbb{Z}_p/\mathcal{P} = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est appelé le *corps résiduel* de $\mathbb{Q}_p$.

Exemple 1.8. Dans un article classique d'Euler où il trouve des relations fonctionnelles pour la fonction ζ de Riemann, il mentionne qu'il n'est pas sans intérêt d'imaginer que la somme

$$1 - 2 + 3 - 4 + 5 - 6 + \cdots,$$

ait la valeur $1/4$. Ceci était justifié avec le développement en série classique

$$\frac{1}{(1+x)^2} = 1 - 2x + 3x^2 - 4x^3 + 5x^4 - 6x^5 + \cdots.$$

De même, en utilisant la série géométrique, Euler serait probablement d'accord avec nous de donner à la somme

$$1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + \cdots,$$

la valeur -1. Or, on sait que ces séries ne convergent pas du tout pour les valeurs dont on est en train de les évaluer, au moins avec la métrique classique. Par contre, cette dernière suite converge sans problème pour la distance 2-adique. De plus, elle converge précisément vers -1. On peut voir cela tout simplement en notant qu'elle est congrue à -1 modulo 2^n pour tout $n \in \mathbb{N}$. Les idées d'Euler reprennent vie alors dans le cadre des corps p-adiques.
Si la série géométrique ne converge pour la valeur absolue réelle que lorsque x est dans l'intervalle $]0, 1[$, on voit qu'il ne se passe pas du tout comme ça pour les corps p-adiques. En effet, on peut démontrer facilement qu'elle converge en $\mathbb{Q}_p$ si et seulement si x est un entier p-adique divisible par p, i.e. si et seulement si $v_p(x) \geq 1$.

1.3 Théorème d'Ostrowski

Après avoir rencontré les corps p-adiques, on pourrait se demander s'il n'y aurait pas d'autres possibles complétions de $\mathbb{Q}$ par rapport à de nouvelles valeurs absolues encore non découvertes. Il n'en est rien : il se trouve qu'avec $\mathbb{R}$ et les $\mathbb{Q}_p$ pour chaque premier p, on a toute la famille, ce qui nous fait utiliser parfois la notation $\mathbb{Q}_\infty := \mathbb{R}$. Ce résultat est dû à Ostrowski, et pour le démontrer il faut d'abord distinguer lorsque deux valeurs absolues donnent la même complétion.

Définition 1.9. On dit que deux valeurs absolues sur un corps K sont *équivalentes* si elles définissent la même topologie sur K.

Notons que c'est bien dans la topologie induite qui se trouve la différence entre deux complétions. Notons aussi qu'il existe encore une valeur absolue que l'on n'a pas mentionnée. Il s'agit de la valeur absolue triviale, i.e. celle qui vaut 0 pour $x = 0$ et qui vaut 1 pour $x \neq 0$. Or, clairement la complétion par rapport à cette valeur absolue n'est que $\mathbb{Q}$ encore une fois.

Proposition 1.10. *Soient $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur un corps K. Les affirmations suivantes sont équivalentes.*

i) $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes ;

ii) $\forall x \in K$, $|x|_1 < 1$ *si et seulement si* $|x|_2 < 1$;

iii) Il existe $\alpha > 0$ *tel que* $\forall x \in K$, $|x|_1 = |x|_2^\alpha$.

Démonstration. Voir [LSW09, Proposition 1.11]. [$\ddot\smile$]

Avec cette proposition, on peut classifier les valeurs absolues sur $\mathbb{Q}$ à équivalence près.

Théorème 1.11 (Ostrowski)**.** *Si on appelle* $|\cdot|_\infty$ *la valeur absolue classique, toute valeur absolue non-triviale sur* $\mathbb{Q}$ *est équivalente à l'une des valeurs absolues* $|\cdot|_p$ *où* p *est un nombre premier ou* ∞.

Démonstration. Voir [LSW09, Théorème 1.12]. [$\ddot\smile$]

Remarque 1.12. On note que les corps $\mathbb{R}$ et $\mathbb{Q}_p$ pour p premier ne sont pas isomorphes entre eux en tant que corps valués (i.e. munis d'une valeur absolue), car une tel isomorphisme devrait fixer $\mathbb{Z}$ et les images de $\mathbb{Z}$ par $|\cdot|_p$ sont clairement différentes pour chaque p premier ou ∞.

1.4 Le principe de Hasse

Ayant maintenant les corps p-adiques (où p est un nombre premier ou ∞) à la main, on a obtenu une infinité de conditions nécessaires en plus pour l'existence d'une solution rationnelle pour un système de polynômes donné. Et sachant que ce sont tous les corps complets que l'on peut obtenir à partir de $\mathbb{Q}$, on pourrait bien se demander si ces conditions sont aussi suffisantes.

Les premières recherches en cette direction au début du XX$^{\text{ème}}$ siècle ont donné des résultats positifs. Les deux théorèmes suivants vont en effet dans la direction d'un algorithme tel qu'on le voudrait. Pour un exposé très élégant de ces résultats, on pourra regarder le livre de Serre [Ser70].

Théorème 1.13 (Minkowski)**.** *Soit* $f(x,y,z) = ax^2 + by^2 + cz^2$ *une forme quadratique sur* $\mathbb{Q}$. *Alors, pour presque tout* p *premier (pour tous sauf un nombre fini),* f *représente* 0 *sur* $\mathbb{Q}_p$, *i.e. il existe un triplet* $(x,y,z) \in \mathbb{Q}_p^3$ *non trivial tel que* $f(x,y,z) = 0$.

Démonstration. Voir [Ser70, Chapitre III, Théorème 3]. [$\ddot\smile$]

On voit alors que pour vérifier si un polynôme quadratique sur $\mathbb{Q}$ a des solutions sur tous ses complétés, il suffit de se concentrer sur une quantité finie d'eux. Et d'après certaines propriétés analytiques des corps p-adiques on peut faire ceci en une quantité finie de pas (il s'agit du lemme de Hensel, voir par exemple [LSW09]). Le résultat suivant nous dit alors qu'on a effectivement un algorithme pour vérifier si un tel polynôme a des solutions sur $\mathbb{Q}$ ou non.

Théorème 1.14 (Minkowski)**.** *Pour toute forme quadratique* f *sur* $\mathbb{Q}$, f *représente* 0 *sur* $\mathbb{Q}$ *si et seulement si elle le fait sur* $\mathbb{Q}_p$ *pour tout* p *premier ou* ∞.

Démonstration. Voir [Ser70, Chapitre IV, Théorème 8]. [$\ddot\smile$]

C'est ce résultat qui est connu comme le *principe de Hasse* pour les formes quadratiques. En général, toute propriété qui soit vérifiée sur $\mathbb{Q}$ si et seulement si elle l'est pour toute complétion de $\mathbb{Q}$ est dite de vérifier ce principe. Plus généralement, pour k un corps de nombres (une extension finie de $\mathbb{Q}$), on peut considérer toutes ses complétions par rapport à une valeur absolue (ce sont des extensions finies de $\mathbb{Q}_p$, dites aussi des corps p-adiques) et le principe de Hasse pour ce corps est défini de la même façon. Hasse a démontré le théorème de Minkowski pour un corps de nombres quelconque en 1921.

Après que ce résultat a été trouvé, des mathématiciens se sont amusés en cherchant s'il pouvait être généralisé à des familles de polynômes plus grandes. Malheureusement, déjà dans le cas des polynômes cubiques cela ne marche plus. Selmer a trouvé en 1951 des familles de contre-exemples à ce joli principe (voir [Sel51]), dont un qui se distingue par sa simplicité.

Théorème 1.15 (Selmer, 1951)**.** *Pour tout p premier et ∞, il existe un triplet $(x, y, z) \in \mathbb{Q}_p^3$ non trivial tel que*

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

Par contre, il n'en existe aucun sur $\mathbb{Q}$, i.e. le principe de Hasse n'est pas vérifié pour ce polynôme.

Vus ces résultats, la réponse à la question posée au début de cette section est donc : non, le principe de Hasse n'arrive que dans des cas très particuliers. La nouvelle tâche était alors d'essayer d'expliquer pourquoi le principe ne marchait pas dans tous ces exemples. C'est le russe Y. Manin qui trouva la première réponse, appelée l'*obstruction de Brauer-Manin*. Mais pour montrer tout cela il faut encore introduire quelques notions.

2 Cohomologie

2.1 Rappels de cohomologie des groupes

On donne ici, pour ceux qui ont fait un peu d'algèbre homologique, un exposé rapide sur la définition de la cohomologie des groupes pour pouvoir passer au cas particulier de la cohomologie galoisienne. Pour un exposé complet sur ces deux théories, on pourra regarder [NSW08] et les livres de Serre [Ser66] et [Ser64].

Pour ceux qui n'ont jamais rencontré la cohomologie, il faut juste garder à l'esprit qu'il s'agit d'invariants des objets étudiés qui servent notamment à communiquer les "défauts" de certaines propriétés qu'ont ces objets. A ce sujet, une citation de Jean-Pierre Serre (qui m'a été communiquée par Étienne Ghys) pourrait aider à éclaircir ceci : "La cohomologie est la différence entre ce que l'on *veut* faire et ce que l'on *peut* faire. Lorsqu'elle est triviale, on est content."

Soit G un groupe et A un G-module, i.e. un groupe abélien avec une action (à gauche) de G "compatible" avec la loi de A au sens suivant : pour $g \in G$ et $a, b \in A$ on a $g\cdot(a+b) = g\cdot a+g\cdot b$. On peut voir A aussi comme un module sur l'anneau $\mathbb{Z}[G]$. Pour un tel A on peut considérer le sous-module A^G des éléments G-invariants. On peut vérifier facilement que le foncteur covariant $F_G : A \mapsto A^G$ est exact à gauche. On alors le droit de dériver ce foncteur.

Définition 2.1. Pour un G-module A et $n \in \mathbb{N}$, on définit le n-ième groupe de cohomologie $H^n(G, A)$ comme le n-ième foncteur dérivé à droite $R^n(F_G, A)$ du foncteur F_G. En particulier, on a $H^0(G, A) = R^0(F_G, A) = A^G$.

On rappelle que d'après la définition des foncteur dérivés à droite, pour toute suite exacte courte de G-modules

$$0 \to A \to B \to C \to 0,$$

on a une suite exacte longue de cohomologie associée :

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \cdots .$$

Les $H^i(G, A)$ pour $i > 0$ sont aussi calculables explicitement à partir de G et A au moyen des *cochaînes*. La formule générale est un peu trop lourde. Par contre, le groupe $H^1(G, A)$ admet une description assez simple. On considère le groupe $Z^1(G, A)$ des 1-*cocycles*, i.e. des fonctions $a : G \to A$ telles que pour tous $g, h \in G$, on a

$$a(gh) = a(g) + g \cdot a(h).$$

On considère aussi le sous-groupe des 1-*cobords*. Ce sont les fonctions $a : G \to A$ telles qu'il existe $b \in A$ tel que

$$a(g) = -b + g \cdot b, \quad \forall g \in G.$$

On peut définir alors $H^1(G, A)$ comme le quotient de $Z^1(G, A)$ par $B^1(G, A)$. On note que lorsque l'action de G sur A est triviale, $H^1(G, A)$ n'est rien de plus que le groupe des homomorphismes $\mathrm{Hom}(G, A)$ à conjugaison près.

Lorsque G est un groupe profini, i.e. une limite projective de groupes finis, on travaille en général avec des G-modules qui ont en plus la propriété que le stabilisateur de chaque élément est ouvert dans G, donc d'indice fini (attention, la réciproque n'est pas forcément vraie). Ceci a la conséquence de que toute orbite de l'action de G est finie. On dit que ces G-modules sont *discrets*. On fait ceci car la catégorie des G-modules discrets est beaucoup plus agréable que celle des G-modules quelconques. De plus, ceci nous permet généralement de nous ramener au cas des groupes finis. En effet,

Proposition 2.2. *Soit G un groupe profini et A un G-module discret. Alors on a*

$$H^n(G, A) = \varinjlim_{H} H^n(G/H, A^H),$$

où H parcourt l'ensemble des sous-groupes de G ouverts distingués.

Démonstration. Voir [NSW08, Proposition 1.5.1]. [⌣̈]

Une notion en cohomologie des groupes qui est très utilisée dans le cadre de la cohomologie galoisienne (qui est celle qui nous intéresse) est celle de dimension cohomologique.

Définition 2.3. Soit G un groupe profini, on appelle *p-dimension cohomologique* et on note $\mathrm{cd}_p(G) \in \mathbb{N} \cup \{\infty\}$ le plus petit entier n tel que pour tout G-module A de torsion on ait $H^i(G, A)\{p\} = 0$ pour tout $i > n$ (où $\{p\}$ veut dire la composante p-primaire du groupe). On définit la *dimension cohomologique* de G comme $\mathrm{cd}(G) := \sup_p \mathrm{cd}_p(G)$.
La *p-dimension cohomologique stricte* $\mathrm{scd}_p(G)$ et la *dimension cohomologique stricte* $\mathrm{scd}(G)$ sont définies de la même façon, à cela près que l'on ne demande pas au G-module A d'être de torsion.

2.2 Cohomologie galoisienne

La cohomologie galoisienne n'est rien de plus que la cohomologie des groupes lorsque G est le groupe de Galois d'une extension algébrique (galoisienne). Ces groupes sont toujours profinis, et l'on fait l'hypothèse que tous les G-modules sont discrets, car dans ce cadre seulement ce type de modules interviennent.

Pour une extension galoisienne K/k de groupe de Galois $G = \mathrm{Gal}(K/k)$ et un G-module discret A, on note souvent $H^i(K/k, A)$ au lieu de $H^i(G, A)$. Dans le cas où K est une clôture algébrique de k, on peut démontrer que le groupe $H^i(K/k, A)$ ne dépend pas du choix de cette clôture. On se permet alors de noter $H^i(k, A)$ pour les groupes de cohomologie correspondants.

Voici quelques résultats de base de cette théorie : deux exemples typiques de G-module sont les groupes abéliens K et K^*. Par rapport à ces modules on a la proposition suivante.

Proposition 2.4. *Pour toute extension galoisienne K/k et tout $i \geq 1$, on a $H^i(K/k, K) = 0$. De plus, on a $H^1(K/k, K^*) = 0$.*

Démonstration. Voir [Ser66, Chapitre X, Propositions 1 et 2] ou [LS10, Propositions 1.3.1 et 1.3.2]. [⌣̈]

L'intêret d'étudier la cohomologie galoisienne dans notre cadre est dû au groupe suivant, qui joue un rôle centrale dans l'obstruction de Brauer-Manin.

Définition 2.5. On définit le *groupe de Brauer* de k comme $\mathrm{Br}(k) := H^2(k, \bar{k}^*)$.

Ce groupe est en fait l'un des objets les plus importants (et compliqués) à étudier dans ce contexte, puisque les groupes de cohomologie de degré supérieur à 2 n'interviennent pas en général. Ceci se voit avec les propositions suivantes.

Proposition 2.6. *Soit p un nombre premier, K un corps p-adique et $G = \mathrm{Gal}(\bar{K}/K)$ son groupe de Galois absolu. Alors la dimension cohomologique de K $\mathrm{cd}(K) := \mathrm{cd}(G) = 2$, et on en a de même pour la dimension cohomologique stricte.*

Démonstration. Pour la dimension cohomologique, voir [Ser64, Chapitre II, Corollaire à la Proposition 12] ou [LS10, Corollaire 1.5.1.1]. Pour la dimension cohomologique stricte, voir [Ser64, Chapitre II, Proposition 15] ou [LS10, Corollaire 1.5.4.1]. [$\ddot\smile$]

La dimension cohomologique d'un corps de nombres se ramène en un certain sens à la cohomologie de ses complétions. Ceci nous permet d'en déduire la proposition suivante.

Proposition 2.7. *Soit k un corps de nombres. Si $p \neq 2$ ou si k est totalement imaginaire (i.e. toute ses complétions ∞-adiques sont isomorphes à $\mathbb{C}$), alors $\mathrm{cd}_p(G) \leq 2$.*

Démonstration. Voir [Ser64, Chapitre II, Proposition 13] ou [LS10, Proposition 1.4.4]. [$\ddot\smile$]

L'hypothèse particulière pour $p = 2$ est due au fait que le groupe de Galois de $\mathbb{R}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, et la 2-dimension cohomologique de ce groupe est infinie.

2.3 Cohomologie étale

La cohomologie des faisceaux en géométrie algébrique a été généralisée d'une façon frappante par les travaux de Grothendieck, notamment grâce à sa nouvelle notion de topologie qui a permis de généraliser celle de Zariski pour un schéma quelconque. Parmi toutes ces nouvelles cohomologies "à la Grothendieck", la cohomologie étale joue un rôle particulier en géométrie arithmétique, car elle correspond à le généralisation naturelle de la cohomologie galoisienne, ce qui nous permet de retrouver la notion de groupe de Brauer pour un schéma quelconque, notamment pour des variétés algébriques.

Il n'est pas nécessaire de donner la définition exacte d'une topologie de Grothendieck pour avoir une idée de ce que c'est la cohomologie étale. En effet, un faisceau de groupes abéliens sur X, au sens classique, n'est qu'un foncteur contravariant $\mathcal{F} : \mathbf{Ouv}(X) \to \mathbf{Ab}$ vérifiant certaines propriétés de recollement. Or, la catégorie $\mathbf{Ouv}(X)$ des ouverts de X est équivalente à la catégorie $\mathbf{Zar}(X)$ des immersions ouvertes $U \to X$. Ce changement de point de vue nous dit qu'il ne faut pas se concentrer sur les ouverts de X en tant qu'espace topoogique, mais sur les morphismes de schémas $Y \to X$ vérifiant certaines propriétés, i.e. sur une certaine famille de X-schémas. La notion d'intersection devient donc celle de produit fibré et la notion d'appartenance est changée par celle de "factorisation du morphisme structural" (et l'on peut vérifier qu'elles coïncident sur les ouverts de X).

Soit donc $\mathbf{Ét}(\mathrm{X})$ la catégorie des schémas étales sur X. Un faisceau étale de groupes abéliens sur X est alors un foncteur contravariant $\mathcal{F} : \text{Ét} \to \text{Ab}$ vérifiant les mêmes propriétés de recollement qu'un faisceau au sens classique. On peut en particulier, pour tout faisceau étale $\mathcal{F}$, considérer les "sections globales" $\mathcal{F}(X)$ de $\mathcal{F}$. C'est en dérivant ce foncteur que l'on définit les groupes de cohomologie étale $H^i_{\text{ét}}(X, \mathcal{F})$.

On peut alors définir le groupe de Brauer d'un schéma comme suit.

Définition 2.8. Soit X une variété algébrique et $\mathbb{G}_m$ le faisceau groupe multiplicatif. C'est le foncteur qui associe au X-schéma étale Y le groupe $\mathcal{O}_Y(Y)^*$. On définit alors le groupe de Brauer de X comme $\mathrm{Br}(X) := H^2_{\text{ét}}(X, \mathbb{G}_m)$.

Remarque 2.9. Ce groupe est souvent appélé le *groupe de Brauer cohomologique* de X. Ceci est dû à une définition plus classique du groupe de Brauer que l'on peut retrouver dans [Ser64, Chapitre X, §5]

On peut démontrer que si X est régulière et K est le corps des fonctions de X, on a alors $\mathrm{Br}(X) \subset \mathrm{Br}(K)$. De plus, le groupe de Brauer est contravariant : un morphisme $Y \to X$ induit un morphisme de groupes $\mathrm{Br}(X) \to \mathrm{Br}(Y)$. En particulier, pour tout L-point $x \in X(L)$, on a une application canonique $\mathrm{Br}(X) \to \mathrm{Br}(L)$.

2.4 L'obstruction de Brauer-Manin

Ayant fait tous les rappels nécessaires, on énonce finalement la grande découverte de Manin qui explique le défaut du principe de Hasse. Cette section est (presque) une traduction de [Sko01, 5.2].

On fixe k un corps de nombres et on note Ω son ensemble de places (pour $k = \mathbb{Q}$, Ω n'est que l'ensemble des nombres premiers plus ∞). On note k_Ω le produit $\prod_{v\in\Omega} k_v$.

Un des résultats fondamentaux de la théorie du corps de classes global est la *loi de réciprocité de Hasse*.

Théorème 2.10 (Brauer-Hasse-Noether)**.** *On a une suite exacte*

$$0 \to \mathrm{Br}(k) \to \bigoplus_{v\in\Omega} \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

où la seconde flèche est l'application diagonale naturelle et la troisième est la somme des invariants locaux $\mathrm{inv}_v : \mathrm{Br}(k_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ donnés par la théorie des corps de classes locaux.

Démonstration. Voir [NSW08, Théorème 8.1.17] [◡̈]

C'est ce résultat que Manin a utilisé pour définir son obstruction au principe de Hasse. Pour cela il définit, pour X une variété lisse, projective et géométriquement intègre, l'accouplement

$$\mathrm{Br}(X) \times X(k_\Omega) \to \mathbb{Q}/\mathbb{Z}, \quad (A, \{x_v\}) \mapsto \sum_{v\in\Omega} \mathrm{inv}_v(A(x_v)),$$

où $A(x_v)$ est l'image de A par l'application canonique $Br(X) \to \mathrm{Br}(k_v)$ induite par le k_v-point x_v. On appelle cet accouplement l'*accouplement de Brauer-Manin*.

Il faut remarquer que la somme dans cette formule est finie. En effet, il existe un ensemble fini $\Sigma \subset \Omega$ tel que X s'étend en un $\mathcal{O}_{k,\Sigma}$-schéma $\mathcal{X}$, et A s'étend alors en un élément de $\mathrm{Br}(\mathcal{X})$. D'autre part, puisque X est projective (donc propre), on a $X(k_\Omega) = X(\mathbb{A}_k)$, i.e. pour toute famille de points $\{x_v\}$ il existe un ensemble fini $\Sigma' \subset \Omega$ tel que pour toute place $v \notin \Sigma' \cup \Sigma$, on ait $X(k_v) = \mathcal{X}(\mathcal{O}_v)$. Ceci nous dit que pour un tel v et un point $x_v \in X(k_v)$, on a $A(x_v) \in \mathrm{Br}(\mathcal{O}_v) = 0$ (c.f. [Mil80, Chapitre IV, §1]). La somme est alors définie sur l'ensemble fini $\Sigma \cup \Sigma'$.

Remarque 2.11. Tout ceci peut être défini dans un cadre plus général. En particulier, X n'a aucun besoin d'être projective (ni propre). Dans ces cas, il faut quand même avoir le soin de prendre le *groupe de Brauer non-ramifié*, qui correspond au groupe de Brauer d'un modèle lisse et propre de X. Il faut aussi prendre les points adéliques $X(\mathbb{A}_k)$ au lieu de $X(k_\Omega)$. Ces points forment ce qu'on appelle un *produit fibré*. C'est le sous-ensemble du produit des éléments (x_v) tels que, pour presque toutes les places (i.e. toutes sauf un nombre fini), on a $x_v \in \mathcal{O}_v$.

Définissons $X(k_\Omega)^{\mathrm{Br}(X)}$ comme le noyau à droite de cet accouplement, i.e. le sous-ensemble de $X(k_\Omega)$ orthogonal à tout élément de $\mathrm{Br}(X)$. La loi de réciprocité de Hasse nous dit que l'image de $X(k)$ par l'application diagonale naturelle $X(k) \hookrightarrow X(k_\Omega)$ est contenu dans $X(k_\Omega)^{\mathrm{Br}(X)}$. Ceci implique que son adhérence est aussi contenue dans cet ensemble.

Définition 2.12. Une variété X comme avant et vérifiant $X(k_\Omega) \neq \emptyset$ alors que $X(k) = \emptyset$ est un *contre-exemple au principe de Hasse*. Ce contre-exemple est pris en compte par l'obstruction de Brauer-Manin si $X(k_\Omega)^{\mathrm{Br}(X)}$ est lui aussi vide.

Remarque 2.13. L'image $\mathrm{Br}_0(X)$ de $\mathrm{Br}(k)$ dans $\mathrm{Br}(X)$ est clairement dans le noyau à gauche de l'accouplement. On peut voir alors l'accouplement comme étant défini sur $\mathrm{Br}(X)/\mathrm{Br}_0(X)$. De plus, parfois on n'a pas besoin de considérer tout le groupe $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ pour trouver des obstructions. Il se trouve que dans pas mal d'exemples il suffit de prendre des sous-groupes B de $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ qui sont plus faciles à calculer et qui vérifient aussi $X(k_\Omega)^B = \emptyset$.

2.5 Un mot sur la cohomologie non abélienne

Soit G un groupe. Par définition, un G-module A doit être un groupe abélien, mais on peut regarder ce qui se passe dans le cas plus général où A est un groupe quelconque avec une action de G "compatible" avec la multiplication dans A. Une telle structure est appelée un G-groupe. Dans ce cas on n'a plus le droit à l'algèbre homologique, car la catégorie des groupes n'est pas une catégorie abélienne. Néanmoins, on peut définir des ensembles pointés de cohomologie $H^i(G, A)$ pour $i = 0, 1$ et obtenir quelques suites exactes avec ces ensembles. Pour un exposé complet de ces notions on pourra regarder les livres de Serre [Ser66, Chapitre VII, Appendice] et [Ser64, Chapitre I, §5] ou bien [LS10, Section 2].

Pour un G-groupe A, le groupe $H^0(G, A)$ est défini tout simplement comme le sous-groupe A^G des G-invariants de A, analoguement au cas abélien. Pour définir $H^1(G, A)$ il faut une petite définition.

Définition 2.14. Soit A un G-groupe. Un *espace principal homogène* (à droite) sur A est un G-ensemble X (i.e. un ensemble sur lequel G agit à gauche) muni d'une action à droite de A qui est libre, transitive et compatible avec l'action de g au sens suivant : pour $g \in G$, $a \in A$ et $x \in X$ on a

$$^g(x \cdot a) = {}^g x \cdot {}^g a.$$

Un morphisme d'espaces principaux homogènes est une application compatible avec les deux actions. On voit facilement qu'une telle application est toujours un isomorphisme.

On définit alors $H^1(G, A)$ comme l'ensemble de classes d'isomorphisme des espaces principaux homogènes sur A. Ce n'est pas du tout un groupe comme dans le cas abélien, mais il a au moins une structure d'ensemble pointé en considérant comme élément distingué la classe de A agissant sur lui-même par multiplication à droite. On peut démontrer facilement que lorsque A est abélien, cet ensemble peut être muni d'une structure de groupe et que ce groupe est canoniquement isomorphe au groupe de 1-cohomologie classique.

Serre avoue dans son livre [Ser64] qu'il ne se risquerait pas en essayant de définir un ensemble de 2-cohomologie non-abélienne. Cela est justifiable car un tel ensemble n'aurait pas de fonctorialité naturelle et même pas une structure d'ensemble pointé en général. Néanmoins, il se trouve que cet ensemble peut être défini quand-même, et ceci d'une façon assez raisonnable lorsqu'on fait les bonnes hypothèses, si l'on change la notion de G-groupe pour une notion un peu plus générale qui est celle de G-lien. Ces notions ont été introduites par Springer dans [Spr66] (on pourra aussi regarder [LS10, Section 2]).

La cohomologie non abélienne est très utile lorsqu'on travaille avec des groupes algébriques sur un corps k. En effet, ces groupes ont une action naturelle du groupe de Galois absolu de k compatible avec la loi de groupe. On a alors le droit de calculer les ensembles de cohomologie non abélienne $H^i(k, G)$ $(i = 0, 1)$ et $H^2(k, G, \kappa)$ pour un groupe algébrique G donné et κ un G-lien. Le groupe $H^0(k, G)$ est notamment le groupe des k-points de G.

3 Espaces homogènes

Parmi les variétés algébriques, les groupes algébriques ont une place particulière à cause de leur structure supplémentaire. L'existence de k-points sur une telle variété est toujours assurée. En effet, l'élément identité d'un tel groupe est toujours défini sur le corps de base. On peut profiter de ce fait et de leur structure de groupe pour étudier l'existence de k-points sur des variétés sur lesquelles ces groupes agissent. Ces variétés font le sujet de cette section.

3.1 Définition et propriétés

Soit X une k-variété munie d'une k-action à droite d'un groupe algébrique G. Ceci veut dire que l'on a un k-morphisme $a : X \times_k G \to X$ qui fait commuter le diagramme suivant

$$\begin{array}{ccc} X \times G \times G & \xrightarrow[a \times \mathrm{id}_G]{} & X \times G \\ {\scriptstyle \mathrm{id}_X \times m}\downarrow & & \downarrow{\scriptstyle a} \\ X \times G & \xrightarrow{\ a\ } & X, \end{array}$$

où m est la multiplication dans G. Pour étudier l'existence d'un k-point sur X, il suffit de le faire sur chaque orbite de cette action. C'est ce qui nous amène à étudier le cas où l'action est transitive, donnant lieu à la définition suivante.

Définition 3.1. Soit G un k-groupe algébrique. Un *espace homogène* sur G est une k-variété X munie d'une k-action de G qui est transitive au niveau des $\overline{k}$-points.

Notons que si l'action est en plus libre, on retrouve les espaces principaux homogènes de la dernière section. Pour ce cas particulier, la question de l'existence d'un k-point est aussi très simple.

Proposition 3.2. *Soit P un espace principal homogène sur G un k-groupe algébrique. En notant $[P]$ la classe de P dans $H^1(k, G)$, on a que P a un k-point si et seulement si $[P]$ est triviale, i.e. elle correspond à l'élément distingué de $H^1(k, G)$.*

Démonstration. On note G' l'espace homogène donné par G agissant sur lui-même par multiplication à droite. Il est clair que si la classe $[P]$ est triviale, alors P à un k-point, puisqu'il est alors k-isomorphe à G' et donc l'image de $1 \in G'$ dans P en est un. En sens inverse, si P a un k-point x, alors on définit un isomorphisme d'espaces homogènes $G' \to P$ par la formule $g \mapsto x \cdot g$. Comme x est défini sur k et l'action de G sur P aussi, le morphisme est bien défini sur k. [ü]

On voit alors que les k-groupes algébriques "idéaux" sont ceux tels que $H^1(k, G) = 0$, car pour ces groupes tout espace principal homogène aurait un k-point. Retournons donc au cas particulier où k est un corps de nombres et regardons ce qui se passe dans ce cas. Pour P un espace principal homogène sur le k-groupe G et pour v une place de k, on peut obtenir par changement de base un espace principal homogène $P_v = P \times_k k_v$ sur le k_v-groupe $G_v = G \times_k k_v$. Comme ceci est valable pour toute place v, on trouve une application

$$H^1(k, G) \to \prod_{v \in \Omega} H^1(k_v, G_v).$$

Supposant que cette application soit injective, il suffirait alors d'étudier ses espaces homogènes "localement", i.e. le principe de Hasse serait vérifié pour eux. En effet, si un espace principal homogène donné a des k_v-points pour tout v, alors il correspond à la classe triviale dans tout $H^1(k_v, G_v)$. L'injectivité de l'application nous dit qu'il correspond aussi à la classe triviale dans $H^1(k, G)$ et il a donc un k-point. Un théorème fondamental qui pointe vers cette direction, dû aux travaux de Harder, Kneser et Chernousov, est le suivant.

Théorème 3.3 (Harder 1965-66, Kneser 1969, Chernousov 1989)**.** *Soit G un k-groupe algèbrique linéaire semisimple simplement connexe. Alors pour toute place finie v de k on a $H^1(k_v, G_v) = 0$. De plus, l'application*

$$H^1(k, G) \to \prod_{v \in \Omega} H^1(k_v, G_v) = \prod_{v \in \Omega_\infty} H^1(k_v, G_v),$$

est un isomorphisme (Ω_∞ étant l'ensemble des places archimédiennes).

On rappelle qu'un groupe semisimple est un groupe tel que son groupe dérivé (le sous-groupe engendré par les commutateurs) est égal à la composante connexe du groupe. En d'autres mots, un tel groupe n'admet pas de quotient abélien non trivial s'il est connexe. On rapelle aussi qu'un groupe algébrique simplement connexe est celui tel que le groupe de ses $\mathbb{C}$-points est une variété simplement connexe au sens topologique. Un exemple classique de ces groupes est $\mathrm{SL}_n(D)$ avec D une algèbre centrale simple.

Démonstration. Voir [PR94, Théorèmes 6.4 et 6.6]. [$\breve{\smile}$]

Remarque 3.4. La preuve de ce théorème repose sur la classification des groupes semisimples simplement connexes. En effet, Kneser a trouvé le résultat pour les groupes classiques, Harder l'a trouvé pour tous les autres, sauf pour le cas du groupe E_8. Chernousov a démontré le résultat pour ce dernier cas particulier 20 ans après. L'existence d'une preuve indépendante de cette classification semble être d'une difficulté très grande.

3.2 Quelques résultats récents et questions à résoudre

Ce dernier résultat est à la base de chaque avancée dans la résolution des questions autour des espaces homogènes. Particulièrement, Mikhail Borovoi s'est basé sur ce résultat et sur une *abélianisation* de la cohomologie non abélienne de sa propre invention (voir [Bor93] et [Bor98] ou bien [LS10]) pour démontrer des résultats sur des espaces homogènes plus généraux, notamment lorsque le stabilisateur d'un point est connexe.

Pour un $\bar{k}$-groupe algébrique linéaire $\bar{H}$, on note $\bar{H}^{\mathrm{u}}$ son radical unipotent et $\bar{H}^\circ$ la composante connexe de l'identité. Le groupe $\bar{H}^{\mathrm{red}} = \bar{H}^\circ/\bar{H}^{\mathrm{u}}$ est alors un groupe réductif. Soit $\bar{H}^{\mathrm{ss}}$ le sous-groupe dérivé de $\bar{H}^{\mathrm{red}}$, alors $\bar{H}^{\mathrm{tor}} = \bar{H}^{\mathrm{red}}/\bar{H}^{\mathrm{ss}}$ est un tore.
Bien que $\bar{H}$ n'admette a priori qu'une action extérieure du groupe $\mathrm{Gal}(\bar{k}/k)$ (i.e. une action à un automorphisme intérieur près), cette action extérieure induit une autre sur $\bar{H}^{\mathrm{tor}}$; et ce groupe étant abélien, cette action extérieure devient une vraie action de groupe qui nous permet de trouver par descente une k-forme canonique H^{tor}.

Théorème 3.5 (Borovoi, 1993)**.** *Soit k un corps de nombres. Soit G un k-groupe semisimple simplement connexe et soit X un espace homogène sur G. Supposons que le stabilisateur $\bar{H}$ d'un point $x \in X(\bar{k})$ est connexe et que*

$$Ш^2(k, H^{\mathrm{tor}}) := \ker[H^2(k, H^{\mathrm{tor}}) \to \prod_{v \in \Omega} H^2(k_v, H^{\mathrm{tor}})] = 0.$$

Alors X vérifie le principe de Hasse.

La nullité du *deuxième groupe de Tate-Shafarevich* $Ш^2(k, H^{\mathrm{tor}})$ est vérifiée dans pas mal de cas. Par exemple, lorsque le tore H^{tor} est quasi trivial, i.e. isomorphe à un produit de groupes de la forme $R_{K/k}\mathbb{G}_m$, où K/k est une extension finie (voir [PR94, 2.1.2] pour la définition de $R_{K/k}G$ pour G un K-groupe). Il est aussi nul lorsque H^{tor} est k_v-anisotrope pour une certaine place v de k, i.e. lorsque le groupe de caractères sur k_v $H^0(k_v, X^*(H^{\mathrm{tor}}))$ est nul. D'autres exemples sont lorsque H^{tor} est de dimension 1, ou bien lorsqu'il est trivial, comme par exemple dans le cas où $\bar{H}$ est semisimple.

Démonstration. Voir [Bor93, Théorème 7.3] ou [LS10, Théorème 5.3.2]. [$\ddot\smile$]

On connait aujourd'hui des espaces homogènes, même principaux, qui ne vérifient pas le principe de Hasse. Serre en construit un explicitement dans [Ser64, Chapitre 3, 4.7], en utilisant un groupe G tel que $H^1(k, G) \neq 0$ (c.f. Proposition 3.2). Néanmoins, pour une bonne quantité d'exemplaires, on sait que l'obstruction de Brauer-Manin associée à un certain sous-groupe de $\mathrm{Br}(X)$ tient compte d'eux. Sansuc a démontré ce résultat dans le cas des espaces principaux homogènes en 1981 (c.f. [San81]). Plus recémment, Borovoi a démontré le même résultat pour une famille beaucoup plus grande d'espaces homogènes, en considérant un sous-groupe particulier de $\mathrm{Br}(X)$ définit comme suit.

Définition 3.6. Soit X une k-variété. On définit son *groupe de Brauer algébrique* $\mathrm{Br}_{\mathrm{al}}(X)$ comme le quotient de $\mathrm{Br}_1(X) := \ker[\mathrm{Br}(X) \to \mathrm{Br}(X_{\bar{k}})]$ par $\mathrm{Br}_0(X) := \mathrm{Im}[\mathrm{Br}(k) \to \mathrm{Br}(X)]$. On définit Б comme le sous-groupe de $\mathrm{Br}_{\mathrm{al}}(X)$ des éléments qui sont localement triviaux, i.e. les $x \in \mathrm{Br}_{\mathrm{al}}(X)$ tels que $x_v \in \mathrm{Br}_{\mathrm{al}}(X_v)$ est nul pour tout $v \in \Omega$.

Le résultat de Borovoi, qui a comme ingrédient de preuve important son théorème précédent, est le suivant.

Théorème 3.7 (Borovoi, 1996)**.** *Soit X un espace homogène sur un k-groupe algébrique linéaire connexe G. On suppose que le noyau de l'application $G \to G^{\mathrm{tor}}$ est aussi connexe et que le stabilisateur $\bar{H}$ d'un point $x \in X(\bar{k})$ est tel que l'image de l'application $\bar{H}^\circ \to \bar{H}^{\mathrm{tor}}$ est abélienne, donc de type multiplicatif. Alors si $X(k_v)$ est non vide pour toute place v de k et si $X(k_\Omega)^{Б} = X(k_\Omega)$, alors X a un k-point.*

Démonstration. Voir [Bor96, Théorème 2.2]. [$\ddot\smile$]

Le théorème comprend les cas où le stabilisateur est soit connexe, soit une extension d'un groupe connexe par un groupe abélien. Suite à ce résultat, il y a donc une question qui se pose naturellement (et que Borovoi a évidemment déjà posé) : qu'est-ce qui se passe pour le cas où le stabilisateur est fini et non abélien ? La réponse à cette question semble être beaucoup plus profonde que les résultats actuels et il semblerait, d'après des travaux de Borovoi et Kunyavskii dans les années 90, que l'obstruction de Brauer-Manin ne suffirait pas pour expliquer le défaut du principe de Hasse dans certains cas.

Dans un cadre plus général, des variétés ne vérifiant pas le principe de Hasse et ce défaut n'étant pas pris en compte par l'obstruction de Brauer-Manin ont déjà été trouvées par Skorobogatov en 1999. Harari et lui-même ont trouvé une généralisation de l'obstruction de Brauer-Manin, appelée *obstruction de descente* qui est présentée dans le livre de Skorobogatov [Sko01]. Elle tenait compte de tous les contre exemples connus jusqu'à 2008, lorsque Poonen trouva un contre exemple à cette obstruction (voir [Poo10]). Une bonne question aujourd'hui est celle de trouver une nouvelle obstruction encore plus générale qui tient compte de ces contre exemples.

Tout ceci nous dit qu'il y a encore pas mal de voies à explorer. On pourrait déjà s'intéresser aux espaces homogènes à stabilisateur fini, voir si l'obstruction de Brauer-Manin y est la seule, et sinon, trouver des nouvelles obstructions comme celle de Skorobogatov, notamment pour le contre exemple de Poonen. Ces études devront sûrement être accompagnées d'études

sur la structure du groupe de Brauer des espaces homogènes, notamment pour trouver des descriptions explicites de certains sous-groupes importants comme Б.

Il y a aussi des études liées à la propriété d'*approximation faible*, qui est la propriété d'une variété X d'avoir ses k-points $X(k)$ comme un sous-ensemble dense de $X(k_\Omega)$. Il s'agit d'une propriété beaucoup plus forte que le principe de Hasse, car elle implique évidement l'existence de k-points dès lors qu'il y a un point dans tous les complétés de k. L'obstruction de Brauer-Manin explique aussi le défaut de cette propriété, mais encore une fois, elle n'est pas forcément la seule. Borovoi a trouvé des résultats similaires à ceux sur le principe de Hasse pour l'approximation faible, mais il reste toujours la question pour les expaces homogènes à stabilisateurs finis non abéliens, où même l'approximation réelle pour $k = \mathbb{Q}$ (i.e. la densité des $\mathbb{Q}$-points dans les $\mathbb{R}$-points) semble être un problème déjà assez compliqué.

Références

[Bor93] Mikhail Borovoi, *Abelianisation of the second nonabelian Galois cohomology*, Duke Math. J. **72** (1993), 217–239.

[Bor96] ———, *The Brauer-Manin Obstruction for homogeneous spaces with connected or abelian stabiliser*, J. Reine Angew. Math. (Crelle) **473** (1996), 181–194.

[Bor98] ———, *Abelian Galois cohomology of reductive groups*, Mem. Amer. Math. Soc. **132** (1998), no. 626.

[Gou00] Fernando Q. Gouvêa, *p-adic numbers*: *an introduction*, 2nd ed., Springer, 2000.

[LSW09] Giancarlo Lucchini Servetto and Li Wang, *Le théorème de Kronecker-Weber local*, Mémoire de Maitrîse, 2009, `http://www.fimfa.ens.fr/fimfa/IMG/File/exposes/2009/lucchini.pdf`.

[LS10] Giancarlo Lucchini Servetto, *Abélianisation de la cohomologie galoisienne non abélienne*, Mémoire de M2, 2010, `http://www.math.u-psud.fr/~lucchini/`.

[Mil80] James S. Milne, *Étale Cohomology*, Princeton University Press, 1980.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of Number Fields*, 2nd ed., A Series of Comprehensive Studies in Mathematics, vol. 323, Springer, 2008.

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic Groups and Number Theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994.

[Poo10] Bjorn Poonen, *Insufficiency of the Brauer-Manin obstruction applied to étale covers*, Annals of Math. **171** (2010), no. 3, 2157-2169, available at `http://www-math.mit.edu/~poonen/papers/insufficiency.pdf`.

[Rob00] Alain M. Robert, *A Course in p-adic Analysis*, 2nd ed., Graduate Texts in Mathematics, vol. 198, Springer, 2000.

[San81] Jean-Jacques Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. Reine Angew. Math. **327** (1981), 12–80.

[Sel51] Ernst S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^2 = 0$, Acta Math. **85** (1951), 203–362.

[Ser70] Jean-Pierre Serre, *Cours d'Arithmétique*, PUF, 1970.

[Ser66] ———, *Local Fields*, 2nd ed., Graduate Texts in Mathematics, vol. 67, Springer, 1966; English transl. in 1980.

[Ser64] ———, *Galois Cohomology*, Springer Monographs in Mathematics, Springer, 1964; English transl. in 1997.

[Spr66] Tonny Albert Springer, *Nonabelian* H^2 *in Galois cohomology*, Sympos. Pure Math. (Boulder, Colo., 1965), Algebraic Groups and Discontinuous Subgroups, 1966.

[Sko01] Alexei Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001.