Mémoire de stage de M2

Elyes Boughattas
Sous la direction d'Olivier Wittenberg

Université d'Orsay

2019

Introduction

Soit k un corps de nombres et Ω_k l'ensemble des places de k. La question suivante apparaît naturellement à quiconque a déjà étudié la théorie de Galois des extensions de corps et s'inscrit dans l'entreprise de description du groupe de Galois absolu du corps $\mathbf{Q}$:

Problème 1 (Problème de Galois inverse)**.** Si G est un groupe fini, existe-t-il une extension galoisienne de k de groupe de Galois G?

L'une des premières approches au problème de Galois inverse a été suggérée par Hilbert et reprise par Noether qui remarqua que la réponse est positive si G admet une k-représentation dont le corps des invariants est rationnel. Toutefois, un premier exemple de groupe dont aucun corps des invariants sur $\mathbf{Q}$ n'est rationnel fut apporté par Xianghao Wang en 1948, à savoir $\mathbf{Z}/8\mathbf{Z}$.

Bien que le programme de Noether ne puisse répondre systématiquement au problème (1), une approche géométrique et englobant celle de Noether est possible. En effet, en faisant agir fidèlement le groupe fini G linéairement sur un espace affine $\mathbf{A}^n_k$ et en notant X le lieu lisse de $\mathbf{A}^n_k/G$, on dit que G vérifie *l'approximation très faible* s'il existe S un ensemble fini de places de k tel que $X(k)$ est dense dans $\prod_{v\in\Omega_k - S} X(k_v)$ et qu'il vérifie *l'approximation faible* si on peut choisir $S = \emptyset$.
Après avoir vérifié que ces propriétés sont indépendantes de la représentation choisie, on peut montrer que si G vérifie l'approximation très faible alors la réponse au problème inverse de Galois est positive pour G. C'est dans ce cadre que Colliot-Thélène conjecture, sous une forme faible:

Conjecture 1 (Colliot-Thélène)**.** Tout groupe fini G vérifie l'approximation très faible.

Quelques exemples de groupes pour lesquels la réponse à cette conjecture est positive sont:

1. Les groupes abéliens (Neukirch, [Neu73]).
2. Les groupes résolubles d'exposant premier au cardinal de $\mu(k)$: dans ce cas on peut prendre $S = \emptyset$ (Neukirch, [Neu79]).
3. Les groupes dits hyper-résolubles (en particulier les groupes nilpotents), c'est-à-dire les groupes G admettant une filtration $\{1\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 \subseteq G_0 = G$ telle que pour tout i on ait $G_i \trianglelefteq G$ et G_{i-1}/G_i qui est cyclique (Harpaz et Wittenberg, [HW18]).

En réalité on peut construire de façon explicite un ensemble fermé BM gisant entre $X(k)$ et $\prod_{v\in\Omega_k} X(k_v)$, appelé l'obstruction de Brauer-Manin, et on dit que l'*obstruction de Brauer-Manin est la seule à l'approximation faible pour G* lorsque $\overline{X(k)} = BM$. Il s'avère que si l'obstruction de Brauer-Manin est la seule à l'approximation faible pour G, alors G vérifie l'approximation très faible. Ceci amène la conjecture plus précise suivante:

Conjecture 2 (Colliot-Thélène)**.** L'obstruction de Brauer-Manin est la seule à l'approximation faible pour tout groupe fini G.

Dans ce mémoire nous étudions le résultat suivant dû à Harari dans [Har07], donné ici sous une forme faible (voir le théorème (7.1) pour l'énoncé plus général):

Théorème A. Si on se donne une suite exacte courte scindée de groupes

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

où A est abélien et l'obstruction de Brauer-Manin est la seule à l'approximation faible pour G, alors il en va de même pour E.

Une conséquence du théorème (A) est que le problème de Galois inverse a une réponse positive pour tout produit semi-direct itéré de groupes abéliens: cette famille de groupes ne s'inscrit dans aucun des exemples sus-indiqués, comme en témoigne l'exemple du groupe alterné $\mathfrak{A}_4$.

La section 0 est destinée à quelques généralités sur les schémas en groupes. Nous y introduisons en particulier les résultats d'existence de quotients pour les actions localement libres de schéma en groupes.

La section 1 rappelle la définition d'un torseur, la classification des torseurs via la cohomologie de Čech ainsi que les opérations de torsion des variétés.

La section 2 est dédiée au groupe de Brauer d'une variété et aux propriétés d'invariances birationnelles de celui-ci entre variétés projectives lisses.

Dans la section 3, nous énonçons le problème de Noether et donnons une démonstration non géométrique de son lien avec le problème de Galois inverse. Il est toutefois à noter qu'on pourrait en fournir une démonstration bien plus courte à la lumière de la section 5.

Nous consacrons la section 4 à une étude plus avancée des propriétés d'approximation faible, très faible et de l'obstruction de Brauer-Manin qui sont apparus sous une forme volubile dans cette introduction. Nous y établissons en particulier le lien entre l'approximation faible et le problème de Grunwald, ce qui nous permet de donner une démonstration au contre-exemple de Wang.

La section 5 est quant à elle dédiée à un énoncé géométrique du théorème de Chebotarev omniprésent en filigrane dans la démonstration du «lemme formel», lequel fait l'objet de la section 6, ainsi que dans la démonstration du théorème (A).

Enfin nous donnons, dans le section 7, la démonstration d'une généralisation du théorème (A) au cadre des groupes algébriques finis.

Remerciements

Je tiens à remercier chaleureusement Olivier Wittenberg pour le temps qu'il a consacré à m'initier à ces belles mathématiques et à répondre à toutes mes questions avec une précision et une clarté bien précieuses.

Je remercie également les organisateurs et les orateurs du trimestre thématique «À la redécouverte des points rationnels» qui s'est déroulé à l'IHP, ainsi que les organisateurs et les participants de l'école d'été intitulée «Galois Theory and Number Theory» qui s'est déroulée à Dresde dans le cadre de l'université franco-allemande. Il va sans dire que ces rendez-vous mathématiques sont tombés à point nommé et m'ont permis d'ouvrir plusieurs horizons.

Enfin, et non des moindres, mes remerciements vont à tous ceux qui de siècle en siècle ont apporté tant aux mathématiques qu'elles sont aujourd'hui si belles.

Notations

Bien que définies au sein du mémoire, on recense, pour le confort du lecteur, les notations récurrentes:

- k: un corps de nombres, sauf mention explicite du contraire.
- Ω_k: ensemble des places de k.
- $\mathbf{A}_k$: anneau des adèles de k.
- Γ_K: groupe de Galois de $K_{\text{sép}}/K$.
- $X(k_S)$: si X est une k-variété et $S \subseteq \Omega_k$ on pose $X(k_S) \coloneqq \prod_{v\in S} X(k_v)$.
- $X(k_\Omega)$: si X est une k-variété, $X(k_\Omega) \coloneqq \prod_{v\in\Omega_k} X(k_v)$.
- $\mathrm{Br}(X)$: le groupe de Brauer cohomologique du schéma X.
- $\mathrm{Br}_0(X)$: si X est une K-variété, $\mathrm{Br}_0(X) \coloneqq \mathrm{Im}\,[\mathrm{Br}(k) \to \mathrm{Br}(X)]$.
- $\mathrm{Br}_1(X)$: si X est une K-variété, $\mathrm{Br}_1(X) \coloneqq \ker\,[\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}})]$.
- $\mathrm{Br}_{\mathrm{nr}}(X)$: groupe de Brauer d'une compactification lisse de X.
- $\mathrm{Pic}(X)$: le groupe de Picard d'un schéma X.

Le lecteur est prié de remarquer que les définitions, propositions, théorèmes, lemmes, corollaires... sont soumis à une numérotation sous la forme $(n.p)$ où l'entier (naturel) n désigne le numéro de la section et l'entier (naturel non nul) p le numéro d'apparition de l'assertion dans ladite section, indépendamment de son type.

Table des Matières

Dans l'ensemble de ce mémoire,
une variété sur un corps K est un K-schéma séparé de type fini.

0 Schémas en groupes

Il est de bon aloi de définir les termes qui apparaissent dans la suite de ce mémoire. Cette section est donc dédiée aux définitions et propriétés fondamentales des schémas en groupes.

On fixe, dans la suite de cette section, un schéma S.

0.1 Définitions

0.1.1 Schémas en groupes

Définition 0.1. Un *S-schéma en groupes* est un foncteur représentable $\mathrm{F} : \mathbf{Sch}/\mathrm{S} \longrightarrow \mathbf{Grp}$. De façon équivalente, c'est un S-schéma G muni de morphismes $\mu : G \times_S G \longrightarrow G$, $e : S \longrightarrow G$ et $i : G \longrightarrow G$ tels que e est un S-point de G et les diagrammes suivants commutent:

$$\begin{tikzcd}
(G \times_S G) \times_S G \simeq G \times_S (G \times_S G) \arrow[r, "id_G \times \mu"] \arrow[d, "\mu \times id_G"'] & G \times_S G \arrow[d, "\mu"] \\
G \times_S G \arrow[r, "\mu"'] & G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "(id_G, i)"] \arrow[dr, "\mu"'] & G \times_S G \arrow[d, "\mu"] & G \arrow[l, "(i, id_G)"'] \arrow[dl, "\mu"] \\
& G &
\end{tikzcd}$$

$$\begin{tikzcd}
G \simeq G \times_S S \arrow[r, "id_G \times e"] \arrow[dr, "id_G"'] & G \times_S G \arrow[d, "\mu"] & S \times_S G \simeq G \arrow[l, "e \times id_G"'] \arrow[dl, "id_G"] \\
& G &
\end{tikzcd}$$

Remarque 0.2. L'équivalence contenue dans la définition est une conséquence immédiate du lemme de Yoneda. Étant donné un S-schéma G, on définit donc à loisir une structure de schéma en groupes soit à travers les morphismes structuraux, soit au niveau de ses S-points.

Définition 0.3. Lorsque S est le spectre d'un corps K, on dit d'un S-schéma en groupes G que c'est un *groupe algébrique* si G est une variété sur K.

Remarque 0.4. En général, si $\mathcal{P}$ est une propriété portant sur les morphismes de schémas et G est un S-schéma en groupes, on dit que G vérifie $\mathcal{P}$ si son morphisme structurel la vérifie.

Définition 0.5. Si G et G' sont des S-schémas en groupes, un *morphisme* de S-schémas en groupes est un S-morphisme $f : G \longrightarrow G'$ tel que $f \circ \mu_G = \mu_{G'} \circ (f, f)$.

Donnons quelques exemples de groupes algébriques qui apparaissent dans la suite:

Exemple 0.6. 1. Soit G un groupe fini. On note G_S le schéma en groupes défini par

$$G_S := \coprod_{g \in G} S \quad , \quad \mu(s_g, s_{g'}) = \mu(s_{gg'}) \quad , \quad i(s_g) = s_{g^{-1}} \quad , \quad e(s_g) = s_e.$$

Ce S-schéma en groupes est appelé le *groupe constant* de type G au-dessus de S.

2. Si $n \geq 0$ et $S = \mathrm{Spec}(A)$ on note GL_n le foncteur qui envoie un S-schéma T sur $\mathrm{GL}_n(\Gamma(T, \mathscr{O}_T))$: il est représenté par le S-schéma $\mathrm{Spec}\left(A\left[\{X_{ij}\}_{1 \leq i,j \leq n}, \det^{-1}\right]\right)$.

0.1.2 Actions de groupes

Définition 0.7. Soit G un S-schéma en groupes dont le morphisme de multiplication est noté μ, le morphisme unité e et X un S-schéma. Une *action* (à gauche) de G sur X est un morphisme $a : G \times_S X \longrightarrow X$ tel que $a \circ (id_G \times a) = a \circ (\mu \times id_X)$ et $a \circ (e \times id_X) = id_X$.

On dit que l'action est *fidèle* si le graphe $\rho : G \times_S X \to X \times_S X$ de l'action est un monomorphisme.

Notations 0.8. Dans la suite de ce mémoire, si G est un K-groupe algébrique agissant sur une variété géométriquement intègre X, on note $K(X)^G$ les éléments de $\overline{K}(X)^{G(\overline{K})}$ invariants sous l'action du groupe de Galois absolu de K.

0.2 Quelques propriétés

0.2.1 Généralités

Commençons par le résultat de lissité suivant, attribué à Cartier:

Théorème 0.9. Tout groupe localement de type fini sur un corps de caractéristique nulle a son morphisme structurel lisse.

Démonstration. [GP11, VIB.1.6.1] □

Nous ferons également appel au fait que tout groupe algébrique fini sur un corps admet une représentation linéaire fidèle de dimension finie:

Théorème 0.10. Si G est un groupe algébrique affine sur un corps K, alors il existe $n \geq 1$ ainsi qu'un morphisme injectif de schémas en groupes $G \hookrightarrow \mathrm{GL}_{n,K}$ qui est une immersion fermée.

Démonstration. [Mil17, corollary 4.10] □

Enfin, pour satisfaire aux hypothèses de quelques théorèmes, nous aurons besoin du résultat suivant dont la démonstration est essentiellement due à Chow:

Théorème 0.11. Un groupe algébrique est quasi-projectif.

Démonstration. [Poo17, theorem 5.2.20.] □

Le fait suivant est utile dans la suite:

Fait 0.12. Soit G un groupe fini étale sur un corps K agissant fidèlement sur une variété géométriquement irréductible X. Alors il existe un ouvert non vide de X stable sous l'action de G et sur lequel G agit librement.

Démonstration. Si G est un groupe constant, pour $g \in G$ notons X^g le lieu des points fixes par g. Alors, le complémentaire de la réunion des X^g pour $g \neq e$ est non vide par irréductibilité et convient.

Si G est fini étale, choisissons K' une extension galoisienne de K telle que $G_{K'}$ est constant. Par le paragraphe précédent, on a un ouvert V de $X_{K'}$ sur lequel $G_{K'}$ agit librement. En notant U' l'intersection des conjugués de V par $\mathrm{Gal}(K'/K)$, on a par descente galoisienne un ouvert U de X tel que $U' = U \otimes_K K'$. Puisque $G_{K'}$ stabilise et agit librement sur U', il vient que G stabilise et agit librement sur U, ce qui conclut. □

0.2.2 Groupes finis étales

Si K est un corps, on note $\overline{K}$ une clôture séparable de K et Γ_K le groupe profini $\mathrm{Gal}\left(\overline{K}/K\right)$. En notant $\Gamma_K\mathrm{-}\mathbf{Ens}_{\mathrm{f}}$ la catégorie des ensembles finis (discrets) munis d'une action continue de Γ_k et $\mathbf{F\acute{E}t}/K$ la catégorie des revêtements étales de $\mathrm{Spec}(K)$:

Théorème 0.13. Les foncteurs

$$\begin{array}{ccc} \mathbf{F\acute{E}t}/K & \rightleftarrows & \Gamma_K\mathrm{-}\mathbf{Ens}_{\mathrm{f}} \\ X & \longmapsto & X(\overline{K}) \\ \mathrm{Spec}\left(\mathrm{Hom}_{\Gamma_K-\mathbf{Ens}}\left(E,\overline{K}\right)\right) & \longleftarrow\!\shortmid & E \end{array}$$

constituent des équivalences de catégorie, pseudo-inverses l'une de l'autre. Ils induisent alors une équivalence entre les catégories des objets en groupes des deux catégories, c'est-à-dire entre la catégorie des groupes finis étales sur K et celle des Γ_K-groupes finis.

Démonstration. L'énoncé est presque tautologique: une démonstration est donnée dans [Poo17, theorem 5.8.1]. □

Enfin, le fait suivant est omniprésent dans la suite:

Fait 0.14. Un morphisme de schémas est fini étale si et seulement s'il est fini et lisse.

Démonstration. Le sens direct étant évident, on s'intéresse au sens réciproque: il suffit de vérifier qu'un morphisme $f : X \longrightarrow S$ fini et lisse est non ramifié. Ceci se vérifie sur les fibres et on peut donc supposer $S = \mathrm{Spec}(k)$ où k est un corps: or puisque f est lisse, on a pour $x \in X$ que $\left[\Omega_{X/S}(x) : \kappa(x)\right] = \dim_x X$ laquelle quantité est nulle car X est de dimension de Krull nulle, puisque f est supposé fini sur k. Ceci étant vrai pour tout x, on en déduit que $\Omega_{X/S} = 0$ et donc que f est non ramifié. □

Le théorème de Cartier, associé au fait précédent, assure donc que:

Corollaire 0.15. Si K est un corps de caractéristique nulle, tout groupe fini sur K est fini étale.

0.2.3 Quotient par un schéma en groupes fini

Définition 0.16. Soit G un S-schéma en groupes et une action $a : G \times_S X \longrightarrow X$. Un *quotient de* X *par* G est un coégalisateur de la paire (a, pr_X) dans la catégorie $\mathbf{Sch}/S$. C'est donc la donnée d'une paire (Y, p), où Y est un schéma sur lequel G agit de façon triviale et $p : X \longrightarrow Y$ est un morphisme de schémas vérifiant $p \circ a = q \circ pr_X$, telle que pour tout morphisme de schémas $q : X \longrightarrow Z$ vérifiant $q \circ a = q \circ pr_X$, il existe un unique morphisme de schémas $\overline{q} : Y \longrightarrow Z$ tel que $q = \overline{q} \circ p$. On note en général le quotient $X/G \coloneqq Y$.

Remarque 0.17.
1. Il faut noter que les coégalisateurs existent dans la catégorie $\mathbf{Ann}/S$ des espaces annelés au-dessus de S: en effet, si $W \underset{g}{\overset{f}{\rightrightarrows}} X$ est une paire de morphismes d'espaces annelés, il suffit de poser Y le quotient de X par la relation d'équivalence engendrée par "$f(x) = g(x)$", de prendre $|p|$ l'application quotient $\pi : X \longrightarrow Y$, de munir Y du faisceau structurel défini comme le sous faisceau de $\pi_* \mathscr{O}_X$ des sections s telles que $f^\#(s) = g^\#(s)$ et de prendre $p^\#$ induit par $\pi^\#$.

2. Néanmoins, la catégorie $\mathbf{Sch}/S$ ne contient pas les coégalisateurs. Mais si le coégalisateur dans $\mathbf{Ann}/S$ de deux morphismes dans $\mathbf{Sch}/S$ est une paire (Y, p) où Y est un schéma et p est un morphisme de schémas, alors (Y, p) est également un coégalisateur dans la catégorie $\mathbf{Sch}/S$.

Un cadre général qui assure l'existence de certains quotients est celui des groupoïdes finis plats qui fait l'objet de [GP11, exposé V, théorème 4.1].

Énonçons ce théorème d'existence dans le cadre qui nous intéresse, à savoir celui d'un groupoïde défini à partir d'une action de groupe, en notant que le point 2 correspond à [GP11, exposé V, remarque 5.1]:

Théorème 0.18. Soit G un S-schéma en groupes et une action $a : G \times_S X \longrightarrow X$. En notant pr_X la projection $G \times_S X \longrightarrow X$, supposons que:

(i) le morphisme pr_X est fini localement libre(1);

(ii) pour tout $x \in X$ l'ensemble $a\left(pr_X^{-1}(x)\right)$ est contenu dans un ouvert affine de X(2).

Alors, le quotient (Y, p) de X par G existe. De plus:

1. le morphisme p est entier et ouvert;

(1)Ceci est équivalent à supposer que a est fini localement libre puisque $a = pr_X \circ \sigma$ où σ est l'automorphisme involutif de $G \times_S X$ défini par $\sigma(g, x) = (g^{-1}, gx)$.

(2)Par la note précédente, $a\left(pr_X^{-1}(x)\right) = pr_X\left(a^{-1}(x)\right)$ et on donc aurait pu remplacer cette hypothèse par: $pr_X\left(a^{-1}(x)\right)$ est contenu dans un ouvert affine de X.

2. si $X \to S$ est quasi-projectif alors $Y \to S$ est également quasi-projectif.

Remarque 0.19. Si $X = \mathrm{Spec}(A)$ est affine et $G = \mathrm{Spec}(H)$ où H est une algèbre de Hopf, une action de G sur H correspond à la donnée d'une structure de H-comodule sur A. Dans ces conditions, on dispose d'une construction explicite du quotient donnée par $X/G = \mathrm{Spec}(A^H)$ et le morphisme p est induit par l'inclusion $A^H \hookrightarrow A$.

Corollaire 0.20. Si G est un schéma en groupes fini sur un corps K agissant sur une variété quasi-projective X, les hypothèses (i) et (ii) du théorème sont satisfaites. Ainsi, le quotient de X par G existe et est quasi-projectif.

Démonstration. L'hypothèse (i) est vérifiée puisque G est supposé fini sur le corps k.

L'hypothèse (ii) est également vérifiée. Tout d'abord, puisque G est quasi-fini sur k, pr_X est quasi-fini. Si x est dans X l'ensemble $E \coloneqq a\left(pr_X^{-1}(x)\right) = pr_X\left(a^{-1}(x)\right)$ est donc une partie finie de X: puisque X est quasi-projectif sur k, l'ensemble E est alors inclus dans un ouvert affine de X[(3)], ce qui conclut. □

Nous avons également besoin par la suite d'une hypothèse de platitude du morphisme quotient. Pour s'en assurer, nous avons besoin du théorème d'existence suivant des quotients par un groupoïde fini plat, qui fait l'objet de [GP11, exposé V, théorème 7.1.] et que nous énonçons là encore dans un cas particulier:

Théorème 0.21. Soit S un schéma localement noethérien, G un S-schéma en groupes et une action $a : G \times_S X \to X$. En notant pr_X la projection $G \times_S X \to X$, supposons que:

(i) le schéma X est quasi-projectif sur S;

(ii) le morphisme pr_X est propre et plat;

(iii) le graphe $G \times_S X \to X \times_S X$ de l'action est quasi-fini.

Alors, le quotient (Y, p) de X par G existe. De plus:

1. le morphisme p est surjectif, ouvert, propre et de présentation finie;
2. le schéma Y est de présentation finie et séparé sur S.

Si en outre on suppose que G agit librement sur X, on conclut également que:

3. le morphisme p est plat.

Les hypothèses (i), (ii) et (iii) étant naturellement vérifiées pour un groupe algébrique fini, on en déduit:

Corollaire 0.22. Si G est un schéma en groupes fini sur un corps K agissant librement sur un variété quasi-projective X, le quotient existe et le morphisme quotient est fppf.

(3) Le fait que tout ensemble fini de points d'un schéma quasi-projectif sur une base affine est contenu dans un ouvert affine est une conséquence du lemme d'évitement homogène.

1 Torseurs

Au cours de cette section, S est un schéma et G un S-schéma en groupes fppf. On introduit ici les définitions et propriétés de base des S-torseurs sous G en soulignant le lien avec la terminologie en cohomologie galoisienne.

1.1 Définition pour une base quelconque

Définition 1.1. Un *S-torseur sous G pour la topologie τ* (encore appelé *G-torseur sur S*) est un S-schéma X muni d'une action (à droite) de G pour lequel il existe un recouvrement $\{U_i \to S\}$ tel que G_{U_i} et X_{U_i}, munis de leur action à droite de G_{U_i}, soient isomorphes (où $G_{U_i} := G \times_S U_i$ et $X_{U_i} := X \times_S U_i$).

Proposition 1.2. Soit X un S-schéma. Les deux conditions suivantes sont équivalentes:

(i) Le morphisme structurel $X \longrightarrow S$ est un morphisme fppf et le morphisme $X \times_S G \longrightarrow X \times_S X$, défini par $(x, g) \mapsto (x, g.x)$, est un isomorphisme.

(ii) Le schéma X est un S-torseur sous G pour la topologie fppf.

Démonstration. L'implication de (ii) par (i) est évidente en prenant le recouvrement $\{X \longrightarrow S\}$.

Pour montrer que (ii) implique (i), commençons par remarquer que l'assertion est Zariski-locale sur S: en particulier, on peut supposer S affine. Donnons-nous un recouvrement fppf $\{U_i \longrightarrow S\}$ (qu'on peut supposer fini puisque S est affine) comme dans l'énoncé et posons $U := \coprod U_i$, si bien que le schéma U est fppf sur S. Enfin, en notant $a : G \times_S X \longrightarrow X \times_S X$ l'action de G sur X, on a par hypothèse que $a \times_S U$ est un isomorphisme et que $G_U \simeq X_U$. Par descente fppf on en déduit que a est un isomorphisme et que X est fppf sur S, ce qui conclut. □

Remarque 1.3.
1. Si $\mathcal{P}$ est une propriété de morphisme vérifiée par le S-schéma G et qui descend via un morphisme fppf alors le S-schéma X vérifie également $\mathcal{P}$. En particulier, si G est lisse sur S alors X aussi.
2. La catégorie des S-torseurs sous G est un groupoïde, comme cela peut aisément se vérifier au niveau des points.
3. Un S-torseur sous G est trivial si et seulement s'il admet une section.

Proposition 1.4. Si G est lisse sur S, alors tout S-torseur X sous G pour la topologie fppf est un torseur pour la topologie étale.

Démonstration. En vertu du point 1. de la remarque (1.3), on dispose d'une trivialisation $\{X \to S\}$ qui est lisse. En vertu de [Gro67, corollaire 17.16.3, (ii)], on dispose d'un morphisme étale surjectif $U \to S$ ainsi que d'un S-morphisme $U \to X$. De là $\{U \to S\}$ est un raffinement de $\{X \to S\}$ qui est étale. Puisque $X \to S$ trivialise X, il en va de même de $U \to S$, ce qui conclut. □

1.2 Description en terme de cohomologie non abélienne

On fixe S un schéma et on note S_{fppf} (resp. $S_{\text{ét}}$) le petit site fppf (resp. étale). Plus généralement, on appelle petit site un site S_τ où $\tau \in \{\text{fppf, lisse, étale, Zariski}\}$.

Définition 1.5. Soit $\mathcal{G}$ un faisceau de groupes et $\mathcal{F}$ un faisceau d'ensembles sur un site $\mathcal{C}$. Une *action* (à droite) de $\mathcal{G}$ sur $\mathcal{F}$ est la donnée d'un morphisme de faisceaux $\mathcal{F} \times \mathcal{G} \longrightarrow \mathcal{F}$ tel que pour tout U l'application $\mathcal{F}(U) \times \mathcal{G}(U) \longrightarrow \mathcal{F}(U)$ définit une action (à droite) de $\mathcal{G}(U)$ sur $\mathcal{F}(U)$.

On dit que $\mathcal{F}$ est un *faisceau de $\mathcal{G}$-torseurs* si pour tout objet U de $\mathcal{C}$, il existe un recouvrement $\{U_i \longrightarrow U\}$ tel que $\mathcal{F}_{U_i}$ et $\mathcal{G}_{U_i}$, munis de leur action à droite de $\mathcal{G}_{U_i}$, soient isomorphes.

Remarque 1.6. Si X est un S-torseur sous G, alors $\text{Hom}_S(-, X)$ est un faisceau de $\text{Hom}_S(-, G)$-torseurs.

Définissons le premier ensemble de cohomologie non abélienne:

Définition 1.7. Soit $\mathcal{G}$ un faisceau de groupes sur un petit site au-dessus de S et $\mathcal{U} = \{U_i \longrightarrow S\}$ un recouvrement de S. Un 1-*cocyle* relativement au recouvrement $\mathcal{U}$ est une famille de $s_{ij} \in \mathcal{G}(U_{ij})$ telle que $s_{ij}s_{jk} = s_{ik}$ sur U_{ijk}. Deux 1-cocyles s et s' sont dits *cohomologues* s'il existe une famille $h_i \in \mathcal{G}(U_i)$ telle que $s'_{ij} = h_i s_{ij} h_j^{-1}$ sur U_{ij}.

L'ensemble pointé des classes de cohomologie (où on distingue la classe de $s_{ij} = 1$) est noté $\check{H}^1(\mathcal{U}, \mathcal{G})$. En passant à la limite inductive on obtient un ensemble pointé noté $\check{H}^1(S, \mathcal{G})$.

La cohomologie non abélienne permet de classifier les faisceaux de torseurs:

Proposition 1.8. On fixe un petit site S_τ sur lequel tous les faisceaux et torseurs sont considérés. Si $\mathcal{G}$ est un faisceau de groupes, on dispose d'un isomorphisme d'ensembles pointés:

$$\{\text{faisceaux de } \mathcal{G}\text{-torseurs}\} / \text{isomorphisme} \xrightarrow{\sim} \check{H}^1_\tau(S, \mathcal{G}).$$

Démonstration. Soit $\mathcal{F}$ un $\mathcal{G}$-torseur et $\mathcal{U} = \{U_i \longrightarrow S\}$ une trivialisation de $\mathcal{F}$. Les isomorphismes $\mathcal{G}_{U_i} \xrightarrow{\sim} \mathcal{F}_{U_i}$ induisent des isomorphismes $\mathcal{G}_{U_{ij}} \xrightarrow{\sim} \mathcal{G}_{U_{ij}}$, lesquelles correspondent à la donnée de $s_{ij} \in \mathcal{G}(U_{ij})$. On vérifie que les s_{ij} sont indépendants du recouvrement fppf et du choix de la trivialisation.

On obtient de la sorte une application

$$\{\text{faisceaux de } \mathcal{G}\text{-torseurs trivialisés par } \mathcal{U}\} / \text{isomorphisme} \longrightarrow \check{H}^1_\tau(\mathcal{U}, \mathcal{G}).$$

qui est clairement injective; la surjectivité est par exemple démontrée dans [Mil80, III, §4, proposition 4.6]. On obtient le résultat souhaité en passant à la limite inductive sur $\mathcal{U}$. □

Si $\mathcal{G}$ est représentable par un groupe G, on dispose des résultats suivants quant à la représentabilité des $\mathcal{G}$-torseurs:

Théorème 1.9. Si G est lisse et séparé sur S avec $\dim S \leq 1$ alors tout faisceau de $\mathcal{G}$-torseurs sur le site fppf est représentable.

Démonstration. [Mil80, III, §4, théorème 4.3] □

Remarque 1.10. Les hypothèses du théorème (1.9) sont satisfaites si G est un groupe algébrique fini sur un corps de caractéristique nulle.

Corollaire 1.11. Sous les hypothèses du théorème (1.9), l'application de la proposition (1.8) induit un isomorphisme d'ensembles pointés

$$\{G\text{-torseurs}\}/\text{isomorphisme} \xrightarrow{\sim} \check{H}^1_{\text{fppf}}(S, G)$$

1.3 Cas où la base est un corps de caractéristique nulle

Fixons K un corps de caractéristique nulle. Le site pris sur $\mathrm{Spec}(K)$ est le site fppf. En vertu du théorème de Cartier et de la proposition (1.4), il est à noter que si G est un K-groupe algébrique alors $\check{H}^1_{\text{fppf}}(\mathrm{Spec}(K), G) \simeq \check{H}^1_{\text{étale}}(\mathrm{Spec}(K), G)$: on note cet ensemble pointé $\check{H}^1(\mathrm{Spec}(K), G)$ ou encore $\check{H}^1(K, G)$, étant sous-entendu que la topologie est la topologie fppf ou étale.

1.3.1 Un lemme géométrique

On énonce ici un fait géométrique souvent passé sous silence dans la littérature et qui permet de ramener l'étude des torseurs sur un corps de caractéristique nulle à celle des espaces homogènes en cohomologie galoisienne. Celui-ci est une conséquence du «Main Theorem» de Zariski:

Fait 1.12. Soit $f : X \longrightarrow Y$ un morphisme de K-variétés où Y est supposée normale. Si f induit une bijection au niveau des $\overline{K}$ points alors c'est un isomorphisme.

1.3.2 Lien avec la cohomologie galoisienne

Le résultat précédent donne une caractérisation intéressante des K-torseurs sous un groupe algébrique:

Proposition 1.13. Soit G un groupe algébrique sur K et X une variété normale sur K sur laquelle G agit. La variété X est un K-torseur sous G si et seulement si $X(\overline{K})$ est un $G(\overline{K})$-espace principal homogène.

Démonstration. Le sens direct est vrai par définition. Pour le sens réciproque, il suffit d'appliquer la proposition (1.12) au graphe de l'action. □

Enfin, si G est un K-groupe algébrique, on peut encore classifier les K-torseurs sous G à l'aide de l'ensemble pointé $H^1(K, G) := H^1(\Gamma_K, G(\overline{K}))$ dont la définition est donnée dans [Ser94, §5.1.]:

Proposition 1.14. On dispose d'un isomorphisme d'ensembles pointés:

$$\{G\text{-torseurs sur } K\}/\text{isomorphisme} \xrightarrow{\sim} H^1(K, G).$$

Démonstration. [Poo17, 5.12.4.] □

1.4 Produit contracté et tordu d'un torseur

On définit le produit contracté de deux schémas sur lesquels agit un schéma en groupe:

Définition 1.15. Soit S un schéma, G un S-schéma en groupes, X et Y des S-schémas sur lesquels G agit respectivement à droite et à gauche. Le *produit contracté de X et Y* est le quotient de $X \times_S Y$ par l'action à droite de G donnée par $(x, y).g = (x.g, g^{-1}.y)$. Lorsqu'il existe, ce quotient est noté $X \times_S^G Y$, ou encore $X \times^G Y$ lorsqu'il n'y a pas d'ambiguïté.

L'existence du produit contracté est assurée par la théorie de la descente:

Proposition 1.16. On reprend les notations de (1.15) en supposant que Y est affine et X un G-torseur à droite. Alors, le produit contracté de X et Y existe.

Démonstration. [Sko01, lemma 2.2.3] □

Notations 1.17. Fixons une base S sur laquelle tous les schémas sont considérés et soit G un S-schéma en groupes. Si X est muni d'une action à droite (resp. à gauche) de G et si $Y \to Z$ est un G_Z-torseur à gauche (resp. à droite) sur S, on note X^Y (resp. ${}_YX$)le produit contracté, s'il existe, de X et Y (resp. Y et X) au-dessus de S, encore appelé *le tordu de X par Y*. Dans ce cas, X^Y (resp. ${}_YX$) est un Z-schéma.

2 Le groupe de Brauer

Dans cette section, K désigne un corps. Commençons par donner la définition du groupe de Brauer d'un schéma:

Définition 2.1. On définit le *groupe de Brauer* (*cohomologique*) d'un schéma X par

$$\mathrm{Br}(X) := H^2_{\text{ét}}(X, \mathbf{G}_m).$$

Par fonctorialité du groupe de Brauer on dispose, si X est une K-variété, de morphismes de groupes $\mathrm{Br}(K) \to \mathrm{Br}(X)$ et $\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}})$. L'image du premier est notée $\mathrm{Br}_0(X)$ et le noyau du second est noté $\mathrm{Br}_1(X)$.

2.1 Quelques généralités

Le lemme suivant est utile dans la suite:

Lemme 2.2. Soit X une k-variété. Pour tout $A \in \mathrm{Br}(X)$, il existe un ensemble fini S de places de k, un $\mathscr{O}_{k,S}$-schéma $\mathcal{X}$ et $\mathcal{A} \in \mathrm{Br}(\mathcal{X})$ tels que X s'identifie à la fibre générique de $\mathcal{X}$ et $\mathcal{A}$ s'envoie sur A via le Brauer du morphisme $X \hookrightarrow \mathcal{X}$.

Démonstration. [Poo17, corollary 6.6.11.] □

On se servira également de la suite exacte suivante:

Théorème 2.3. Soit X une variété géométriquement intègre et lisse sur un corps K de caractéristique nulle. En notant $\overline{X} := X \otimes_K \overline{K}$ et en supposant que $\mathrm{Br}(\overline{X}) = 0$, on a une suite exacte:

$$\mathrm{Br}_0(X) \longrightarrow \mathrm{Br}_1(X) \longrightarrow H^1(K, \mathrm{Pic}(\overline{X})) \longrightarrow H^3(K, \mathbf{G}_m) \longrightarrow H^3(X, \mathbf{G}_m)$$

Démonstration. [Sko01, corollary 2.3.9.] □

On donne ensuite une série de théorèmes qui permettent de mieux appréhender la structure du groupe de Brauer d'une variété intègre lisse:

Théorème 2.4. Si X est un schéma intègre régulier, alors le morphisme $\mathrm{Br}(X) \to \mathrm{Br}(K(X))$ donné par le point générique est injectif.

Démonstration. Si U est un ouvert de X, la proposition (2.8) assure que le morphisme $\mathrm{Br}(X) \to \mathrm{Br}(U)$ est injectif. On en déduit que le morphisme naturel $\mathrm{Br}(X) \to \varinjlim_{U \text{ ouvert}} \mathrm{Br}(U)$ est injectif. Or on a

$$\varinjlim_{U \text{ ouvert}} \mathrm{Br}(U) = \mathrm{Br}\left(\varprojlim_{U \text{ ouvert}} U\right) = \mathrm{Br}(\mathrm{Spec}(k(X)) = \mathrm{Br}(k(X))$$

ce qui conclut. □

Théorème 2.5. Soit R un anneau de valuation discrète, de corps des fractions K et de corps résiduel κ. On suppose que K est de caractéristique nulle et que κ est un corps parfait. On dispose alors d'une suite exacte:

$$0 \longrightarrow \mathrm{Br}(R) \longrightarrow \mathrm{Br}(K) \xrightarrow{\delta} H^1(\kappa, \mathbf{Q}/\mathbf{Z})$$

où δ est appelé le *morphisme de résidu*.

Théorème 2.6. Si X est un schéma régulier, intègre, dont les corps résiduels sont parfaits, on dispose d'une suite exacte

$$0 \longrightarrow \mathrm{Br}(X) \longrightarrow \mathrm{Br}(K(X)) \xrightarrow{\sum \delta_x} \bigoplus_{x \in X^{(1)}} H^1(\kappa(x), \mathbf{Q}/\mathbf{Z})$$

où le morphisme $\delta_x : \mathrm{Br}(k(X)) \to H^1(\kappa(x), \mathbf{Q}/\mathbf{Z})$ est appelé *morphisme de résidu en x.*

Démonstration. [Mil80, chapter III, §2, example 2.22.] □

Dès que L/K est une extension de corps, on pose

$$\mathrm{Br}_{\mathrm{nr}}(L/K) \coloneqq \bigcap_{K \subseteq R \subseteq L \text{ avd}} \mathrm{Br}(R) \subseteq \mathrm{Br}(L).$$

2.2 Groupe de Brauer comme invariant de variétés projectives lisses

Soit K un corps. Le critère d'invariance birationnelle suivant est donné dans [Voi19, lemma 1.1.]:

Lemme 2.7. Soit A un foncteur contravariant, de la catégorie des variétés lisses sur K dans celle des groupes abéliens. Considérons les assertions:

(i) Si U est un ouvert dense de X, alors $A(X) \to A(U)$ est injective.

(ii) Si U est un ouvert de X tel que $\mathrm{codim}(X - U) \geq 2$, alors $A(X) \to A(U)$ est un isomorphisme.

Si (i) et (ii) sont vérifiées, alors A est un invariant birationnel de variétés projectives lisses.

Démonstration. [Voi19, lemma 1.1.] □

En vue d'appliquer ce lemme aux groupes de Brauer, on est amené à montrer que les deux hypothèses de 2.7 sont vérifiées:

Proposition 2.8. Soit X un schéma régulier et U un ouvert dense de X. Alors l'inclusion $U \hookrightarrow X$ induit une injection $\mathrm{Br}(X) \hookrightarrow \mathrm{Br}(U)$.

Démonstration. Notons $j : U \hookrightarrow X$ l'inclusion de U dans X. La suite spectrale de Leray associée à j s'écrit:

$$E_2^{p,q} = H^p(X, \mathcal{R}^q j_* \mathbf{G}_m) \Rightarrow H^{p+q}(U, \mathbf{G}_m)$$

d'où on déduit le fragment suivant de la suite exacte à cinq termes:

$$H^0(X, \mathcal{R}^1 j_* \mathbf{G}_m) \longrightarrow H^2(X, j_* \mathbf{G}_m) \longrightarrow \mathrm{Br}(U).$$

Commençons par montrer que $H^0(X, \mathcal{R}^1 j_* \mathbf{G}_m) = 0$. En effet, $\mathcal{R}^1 j_* \mathbf{G}_m = 0$ car si $\overline{x}$ est un point géométrique, alors

$$(\mathcal{R}^1 j_* \mathbf{G}_m)_{\overline{x}} = H^1((\mathrm{Spec}(\mathscr{O}_{X,\overline{x}}))^{\mathrm{sh}} \times_X U, \mathbf{G}_m) = \mathrm{Pic}((\mathrm{Spec}(\mathscr{O}_{X,\overline{x}}))^{\mathrm{sh}} \times_X U)$$

Or, $\mathrm{Pic}((\mathrm{Spec}(\mathscr{O}_{X,\overline{x}}))^{\mathrm{sh}}) \twoheadrightarrow \mathrm{Pic}((\mathrm{Spec}(\mathscr{O}_{X,\overline{x}}))^{\mathrm{sh}} \times_X U)$ et $\mathrm{Pic}((\mathrm{Spec}(\mathscr{O}_{X,\overline{x}}))^{\mathrm{sh}}) = 0$ d'où il vient que $(\mathcal{R}^1 j_* \mathbf{G}_m)_{\overline{x}} = 0$ et donc que $\mathcal{R}^1 j_* \mathbf{G}_m = 0$. En particulier, le morphisme $H^2(X, j_* \mathbf{G}_m) \to \mathrm{Br}(U)$ est injectif.

De plus, l'application $H^2(X, \mathbf{G}_m) \to H^2(X, j_* \mathbf{G}_m)$ est également injective. En effet, posons pour $x \in X^{(1)} - U$ le morphisme $i_x : \mathrm{Spec}(\kappa(x)) \to X$. Alors, la suite suivante est exacte:

$$0 \longrightarrow \mathbf{G}_m \longrightarrow j_* \mathbf{G}_m \longrightarrow \bigoplus_{x \in X^{(1)} - U} i_{x,*} \mathbf{Z} \longrightarrow 0.$$

De plus, les $H^1(X, i_{x,*}\mathbf{Z})$ sont nuls car le début de la suite exacte à cinq termes associée à i_x donne une suite exacte:

$$0 \longrightarrow H^1(X, i_{x,*}\mathbf{Z}) \longrightarrow H^1(\mathrm{Spec}(\kappa(x)), \mathbf{Z})$$

où $H^1(\mathrm{Spec}(\kappa(x)), \mathbf{Z}) = H^1(\mathrm{Gal}(\overline{\kappa(x)}/\kappa(x)), \mathbf{Z}) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\kappa(x)}/\kappa(x)), \mathbf{Z}) = 0$. □

Le résultat suivant est plus connu sous le nom de théorème de pureté de Grothendieck:

Théorème 2.9 (théorème de pureté)**.** Soit K un corps de caractéristique nulle et X une variété lisse sur K. Si U est un ouvert de X tel que $\mathrm{codim}(X - U) \geq 2$, alors l'inclusion $U \hookrightarrow X$ induit un isomorphisme $\mathrm{Br}(X) \simeq \mathrm{Br}(U)$.

Démonstration. En donner une démonstration ici détournerait le lecteur du sujet d'étude. On renvoie à [GGK+68, §6]. □

On en déduit donc que le groupe de Brauer est un invariant de variétés projectives lisses:

Théorème 2.10. Si X et Y sont des variétés projectives lisses birationnelles sur un corps de caractéristique nulle, alors

$$\mathrm{Br}(X) \simeq \mathrm{Br}(Y).$$

Remarque 2.11. Il convient de remarquer cet isomorphisme n'est pas quelconque. Dans un premier temps, se donner une application birationnelle entre X et Y revient à se donner des isomorphismes entre les corps des fonctions des différentes composantes connexes de X et de Y: on se ramène donc au cas ou X et Y sont irréductibles. Dans ce cas, l'application birationnelle correspond à un isomorphisme entre $k(X)$ et $k(Y)$ et donc à un isomorphisme $\alpha : \mathrm{Br}(k(X)) \xrightarrow{\sim} \mathrm{Br}(k(Y))$. Ce que dit le théorème est que α induit un isomorphisme entre $\mathrm{Br}(X)$ et $\mathrm{Br}(Y)$, où $\mathrm{Br}(X)$ (resp. $\mathrm{Br}(Y)$) est identifié à un sous-groupe de $\mathrm{Br}(k(X))$ (resp. $\mathrm{Br}(k(Y))$) via le théorème (2.4).

2.3 Groupe de Brauer non ramifié

2.3.1 Définition

Pour pouvoir définir le groupe de Brauer non ramifié, l'essentiel du travail a été fait dans les sections précédentes. Commençons par énoncer le résultat de compactification lisse suivant, qui est une combinaison d'un résultat de résolution des singularités, dû à Hironaka, et d'un théorème de compactification de Nagata.

Théorème 2.12. Si K est un corps de caractéristique nulle et X une K-variété lisse, il existe une K-variété propre lisse X' ainsi qu'une immersion ouverte $X \hookrightarrow X'$. On dit que X' est une *compactification lisse* de X.

Démonstration. [Hir64] $\square$

En combinant les théorèmes (2.12) et (2.10), il suit que si X vérifie les hypothèses de (2.12), alors le groupe de Brauer d'une compactification lisse est indépendant du choix de cette dernière, ce qui justifie la définition suivante:

Définition 2.13. Soit X une variété sur un corps de caractéristique nulle et X' une compactification lisse du lieu lisse de X. Alors on définit le *groupe de Brauer non ramifié* de X comme suit:

$$\mathrm{Br}_{\mathrm{nr}}(X) := \mathrm{Br}(X').$$

2.3.2 Quelques propriétés

Le théorème de pureté de Grothendieck permet de décrire le groupe de Brauer non ramifié d'une variété intègre lisse au sein du groupe de Brauer de son corps de fonctions:

Théorème 2.14. Si X est une variété intègre et lisse sur un corps K de caractéristique nulle, l'image du morphisme $\mathrm{Br}_{\mathrm{nr}}(X) \hookrightarrow \mathrm{Br}(K(X))$ est égale à $\mathrm{Br}_{\mathrm{nr}}(K(X)/K)$

Démonstration. [GGK$^+$68] $\square$

On dispose également d'une propriété de fonctorialité pour le groupe de Brauer non ramifié:

Proposition 2.15. Si $f : X \to Y$ est un morphisme dominant de variétés lisses et intègres sur un corps de caractéristique nulle, alors $f^* : \mathrm{Br}(Y) \to \mathrm{Br}(X)$ envoie $\mathrm{Br}_{\mathrm{nr}}(Y)$ sur $\mathrm{Br}_{\mathrm{nr}}(X)$.

Démonstration. [CTS07, lemma 5.5.] $\square$

3 Première approche au problème de Galois inverse: le théorème de Noether

En reprenant un résultat de Hilbert, Emmy Noether a démontré dans [Noe17] un premier critère de réalisation d'un groupe fini comme groupe de Galois au-dessus d'un corps de nombres:

Théorème 3.1. [Hilbert-Noether] Soient k un corps de nombres, G un groupe fini et V une représentation fidèle de G. Si $k(V)^G$ est rationnel sur k alors G est le groupe de Galois d'une extension galoisienne de k.

Dans l'optique du problème de Galois inverse, ce théorème soulève alors une interrogation assez générale connue sous le nom de *problème de Noether*: le corps des invariants d'une représentation fidèle d'un groupe fini est-il rationnel?

Wang a donné un exemple où le corps des invariants n'est pas rationnel. Néanmoins, ce contre-exemple de Wang n'est pas présenté dans cette section et apparaît naturellement dans la section 4 où le problème de Noether est relié au théorème de Grunwald via des considérations générales sur l'approximation faible.

Dans cette section, nous donnons une démonstration *ad-hoc* du théorème (3.1) en suivant [Swa83]: pour ce faire, nous devons admettre le théorème d'irréductibilité de Hilbert sous sa forme faible, qui fait l'objet du théorème (3.10).

À noter qu'il serait possible de donner une démonstration plus courte en disposant de la forme forte du théorème de Hilbert qui assure l'existence d'une spécialisation de même groupe de Galois que le polynôme général: en réalité, ce résultat est tout à fait accessible en utilisant le lemme d'Ekedahl de la section 5 mais nous faisons le choix de ne pas le démontrer. Le lecteur est néanmoins invité à se référer à [Eke90, theorem 1.3.].

3.1 Éléments de théorie de Galois des anneaux commutatifs

Dans cette sous-section, tous les anneaux sont commutatifs, unitaires.

Définition 3.2. Soient $A \subseteq B$ des anneaux et G un groupe fini d'automorphismes de B. On dit que B est une extension galoisienne de A de groupe G si

(i) $A = B^G$;

(ii) Si $H \leq G$ et I est un idéal propre de B stable par H, alors H agit fidèlement sur B/I.

On dispose de plusieurs caractérisations équivalentes du caractère galoisien d'une extension d'anneaux:

Proposition 3.3. Soit G un groupe fini d'automorphismes d'un anneau B et $A := B^G$. Les assertions suivantes sont équivalentes:

1. B est une extension galoisienne de A de groupe de Galois G.

2. Il existe $x_i, y_i \in B$ tels que pour tout $\sigma \in G$ on ait $\sum_i x_i\sigma(y_i) = \delta_{\sigma,1}$ où δ désigne le symbole de Kronecker.

3. Le morphisme de A-algèbres $h : B\otimes_A B \longrightarrow \prod_{\sigma\in G} B$ défini par $b\otimes b' \mapsto (b\sigma(b'))$ est un isomorphisme.

Démonstration. Le fait que 2. implique 1. est élémentaire.

Pour montrer que 1. implique 2., il suffit de définir pour chaque σ l'idéal I engendré par les $\sigma(b)-b$ pour b dans B: puisque σ stabilise I et agit trivialement sur B/I, on en déduit que $I = B$ et donc qu'on a $a_i, b_i \in B$ tels que $\sum_i a_i(b_i-\sigma(b_i)) = 1$. En posant $a_0 := 1 - \sum_i a_ib_i$, $b_0 := 1$ puis $z_\sigma := \sum_{0,i} a_ib_i$ on en déduit que $h_1(z_\sigma) = 1$ et $h_\sigma(z_\sigma) = 0$ (où, pour $\tau \in G$, on note h_τ la composition de la projection suivant τ de $\prod_{\sigma\in G} B$ par h). En posant $z = \prod_\sigma z_\sigma = \sum x_i \otimes y_i$ on en déduit que $h(z) = (1, 0, \dots, 0)$ et donc que les x_i et les y_i conviennent.

Pour montrer que 3. implique 2. il suffit de prendre $z = \sum_i x_i \otimes y_i \in B \otimes_A B$ un antécédent de $(1, 0, \dots, 0)$ si bien que les x_i et les y_i conviennent.

Enfin, pour montrer que 2. implique 3., on prend des x_i et des y_i comme dans 2. et on vérifie que $k : \prod_{\sigma\in G} B \longrightarrow B\otimes_A B$ définie par $k\left((b_\sigma)\right) := \sum_\sigma \sum_i x_i\otimes\sigma^{-1}(y_ib_\sigma)$ est un inverse de h. □

Notons $tr : B \longrightarrow A$ définie par $\mathrm{tr}(b) := \sum_\sigma \sigma(b)$. On déduit du point 2. de la proposition (3.3) le:

Corollaire 3.4. Si $A \subseteq B$ est galoisienne de groupe G alors B est un A-module projectif de type fini.

Démonstration. Se déduit du fait que l'identité de B se décompose en $B \longrightarrow A^n \longrightarrow B$ où la première flèche est donnée par $b \mapsto (\mathrm{tr}(by_i))$ et la deuxième par $(a_i) \mapsto \sum_i x_ia_i$. □

Enfin, on dispose des résultats suivants:

Proposition 3.5. Si B est une extension galoisienne de A alors $tr : B \longrightarrow A$ est surjective et l'accouplement $\langle\, ,\rangle : B\times B \longrightarrow A$ défini par $\langle b, b'\rangle = \mathrm{tr}(bb')$ est parfait.

Démonstration. Notons que $\mathrm{tr}(B)$ est un idéal de A, noté I, tel que $IB = B$: en effet $b = \sum_i x_i \,\mathrm{tr}(by_i)$. Puisque B est un A-module de type fini, le lemme de Nakayama donne $a \in I$ tel que pour tout b dans B on a $b = ab$: avec $b = 1$ on en déduit que $1 \in I$ et donc que $I = A$ et que tr est surjective.

De plus, pour vérifier que l'accouplement est parfait, il suffit par descente fidèlement plate de le vérifier dans la cas où $B = \prod_\sigma A$ où G agit sur $\prod_\sigma A$ par $\sigma.(a_\tau) := (a_{\tau\sigma})$. Dans ce cas, on vérifie aisément que l'accouplement est parfait. □

Proposition 3.6. Si B est une extension galoisienne de A de groupe G et C une A-algèbre alors $C \otimes_A B$ est une extension galoisienne de C de groupe G.

Démonstration. Puisque $A \longrightarrow B$ admet une rétraction donné par $b \mapsto \mathrm{tr}(bc)$, où c est de trace 1, on en déduit que $C \longrightarrow C \otimes_A B$ est injective. En faisant agir G sur $C \otimes_A B$ sur le second facteur on a donc que $(C \otimes_A B)^G \subseteq C \otimes_A B$ vérifie le point

2. de la proposition (3.3) car il en va de même de $A \subseteq B$: ainsi $C \otimes_A B$ est une extension galoisienne de $(C \otimes_A B)^G$ de groupe G. De là

$$(C \otimes_A B)^G = tr\,(C \otimes_A B) = C \otimes_A \mathrm{tr}(B) = C$$

où la première et le dernière égalité découlent de la proposition (3.5). $\square$

Le lemme suivant apparaîtra dans la section suivante dans le cas d'une extension de corps galoisienne, auquel cas il est plus connu sous le nom de lemme de Speiser. Nous en donnons ici un énoncé qui vaut dans le cadre général de cette sous-section:

Proposition 3.7. Soit $A \subseteq B$ une extension galoisienne de groupe G et M un B-module muni d'une G-action semi-linéaire. Alors le morphisme $B \otimes_A M^G \longrightarrow M$ défini par $b \otimes m \mapsto bm$ est un isomorphisme.

Démonstration. Quitte à tensoriser par B puis à raisonner par descente fidèlement plate, le point 3. de la proposition (3.3) permet de se ramener au cas où $B = \prod_{\sigma \in G} A$ et où G agit sur $\prod_{\sigma \in G} A$ par $\sigma.(a_\tau) := (a_{\tau\sigma})$. En tant que A-module, on a donc une décomposition de M sous la forme $M = \bigoplus_\sigma M_\sigma$ où $M_\sigma = (\delta_{\sigma\tau})M$ et l'action de $\prod_{\sigma \in G} A$ sur M est donnée par $a_\sigma m_\tau = a m_{\sigma\tau}$. On en déduit que $M^G = M_1$ et donc que $B \otimes_A M^G = B \otimes M_1 \simeq M$, ce qui conclut. $\square$

Lemme 3.8. Soit L/K une extension finie galoisienne de corps de groupe G. Soit $B \subseteq L$ un sous-anneau stable par G, de corps des fractions L et posons $A = B^G$. Alors il existe s dans A non nul tel que $B\left[s^{-1}\right]$ est une extension galoisienne de $A\left[s^{-1}\right]$ de groupe G.

Démonstration. Pour $s \in A$ non nul, b/s^n est fixe par G si et seulement b l'est, d'où on déduit que $B\left[s^{-1}\right]^G = A\left[s^{-1}\right]$. Soient x_i, y_i dans L tels que dans la proposition (3.3) et $t \in B$ tel que $x_i, y_i \in B\left[t^{-1}\right]$: il suffit alors de poser $s = \prod_\sigma \sigma(t)$. $\square$

À toute extension galoisienne B de groupe G d'un anneau A et tout sous-groupe H de G on peut associer une extension galoisienne induite de A comme suit.

On pose $Ind_H^G(B) := \mathrm{Hom}_{A[H]}\left(A\left[G\right], B\right)$ qui est un anneau contenant A et sur lequel G agit par $(\sigma.f)(\tau) := f(\tau\sigma)$; il est alors clair que $Ind_H^G(B)^G = A$. En outre, si on se donne x_i, y_i associés à l'extension B de A comme dans le point 2. de la proposition (3.3), si on note (τ_k) une famille de représentants des classes de G par H et si on pose $f_{ij}(\tau_k) := \delta_{jk}x_i$ et $g_{ij}(\tau_k) := \delta_{jk}y_i$, alors pour $\sigma \in G$ on a $\sum_{i,j} f_{ij}\sigma\left(g_{ij}\right) = \delta_{\sigma,1}$. Ainsi $Ind_H^G(B)$ est une extension galoisienne de A de groupe G.

Toute extension galoisienne sur un corps est induite par une extension galoisienne de corps:

Proposition 3.9. Soit B une extension galoisienne d'un corps K de groupe G. Alors il existe un sous-groupe H de G et une extension galoisienne L de K de groupe H telle que $B \simeq Ind_H^G(L)$.

Démonstration. Soit J le radical de B. Commençons par remarquer que $J = 0$: en effet, si $J \neq 0$ on a un idéal G-stable I de B non nul tel que $I^2 = 0$ (prendre $I = J^n$ où $n+1$ est l'ordre de nilpotence de J) ce qui contredit la bijectivité de l'application h définie au point 3. de la proposition (3.3) car $I \otimes I \neq 0$ tandis que $h(I \otimes I) = 0$.

Puisque $J = 0$, il vient que que B est un produit de corps $L_1 \times \cdots \times L_n$. Puisque G permute les idéaux maximaux de B, il permute également les L_i: si on note H le stabilisateur de $L := L_1$ alors on vérifie aisément que $B \simeq Ind_H^G(L)$. $\square$

3.2 Démonstration du théorème de Noether

La démonstration repose sur une version faible du théorème d'irréductibilité de Hilbert qu'on admettra:

Théorème 3.10. Soit k un corps de nombres, $K = k\,(x_1, \ldots x_n)$ et $f \in K\,[T]$ un polynôme irréductible sur K. Il existe alors $a_1, \ldots, a_n \in k$ tels que $f(a_1, \ldots, a_n, T)$ est défini et irréductible.

Démonstration. [Ser97, section 9.6.] $\square$

Donnons-nous k, G et V une représentation fidèle de G comme dans l'énoncé du théorème (3.1). Commençons par un fait *ad hoc*:

Fait 3.11. Soit L/K une extension galoisienne de corps de groupe G et B un sous-anneau de L de corps de fractions L tel que B/A est une extension galoisienne de groupe G, où $A := B^G$. Écrivons $L = K\,[\alpha]$ avec $\alpha \in B$ de polynôme minimal $f \in A\,[T]$. Si $\phi : A \longrightarrow M$ est un morphisme d'anneaux où M est un corps et si $\phi(f)$ est irréductible sur M alors $M \otimes_A B$ est un corps.

Démonstration. Posons $n = \deg f$, $g = \phi(f)$ et supposons que g est irréductible de degré. Notons alors que $1 \otimes \alpha \in M \otimes_K L$ engendre le corps $M\,[T]\,/(g)$ avec $n = [M\,[T]\,/(g) : M]$. Or on a également $n = [M \otimes_K L : M]$ car $M \otimes_K L$ contient $M\,[T]\,/(g)$, donc est de dimension au moins n, et d'après la démonstration du corollaire (3.4) $M \otimes_K L$ est de dimension au plus $|G| = n$. On en déduit que $M \otimes_K L = M\,[T]\,/(g)$ est un corps. $\square$

Posons $L = k(V)$ et $K = k(V)^G$ et quitte à spécifier une base de V, écrivons $L = k(x_1, \ldots, x_n)$ et $K = k(x_1, \ldots, x_n)^G$. Le lemme (3.8) permet de choisir $B \subseteq L$ de type fini sur k, de corps des fractions L et $A \subseteq K$ tels que B est une extension galoisienne de A de groupe G. Soit également $\alpha \in B$ tel que $L = K\,[\alpha]$ et $f \in A\,[T]$ son polynôme minimal sur K.

Puisque B est de présentation finie sur k et de type fini sur A par le corollaire 3.4., il vient que A est de type fini sur k: on a donc $h \in k\,[x_1, \ldots, x_n]$ tel que $A \subseteq k\,[x_1, \ldots, x_n, h^{-1}]$. En appliquant le théorème (3.10) à f/h, on dispose donc de $a_1, \ldots, a_n \in k$ tels que $h(a_1, \ldots, a_n) \neq 0$ et $f(a_1, \ldots, a_n, T)$ est irréductible sur k.

On applique alors le fait (3.11) au morphisme $\phi : A \longrightarrow k$ donné par l'inclusion $A \subseteq k\,[x_1, \ldots, x_n, h^{-1}]$ suivie de la spécialisation $x_i \mapsto a_i$: on en déduit que $k \otimes_A B$ est une extension galoisienne de corps de k de groupe G, ce qui conclut.

4 Une autre approche via des questions d'approximation

Dans cette section k désigne un corps de nombres et G un groupe algébrique fini sur k. Notons k_Ω l'ensemble des places de k.

4.1 L'approximation faible et très faible

Commençons par remarquer que pour tout ensemble $S \subseteq k_\Omega$ on dispose d'une application d'ensembles pointés:

$$\varphi_S : H^1(k, G) \longrightarrow \prod_{v \in S} H^1(k_v, G)$$

Définition 4.1.

1. Si $S \subseteq k_\Omega$, on dit que G *vérifie l'approximation faible pour* S si φ_S est surjective.

2. On dit que G *vérifie l'approximation faible* si pour tout ensemble fini S de places, G vérifie l'approximation faible pour S. On abrégera ceci en disant que «G vérifie (AF)».

3. On dit que G *vérifie l'approximation très faible* s'il existe un ensemble fini S_0 de places de k tel que pour tout ensemble fini S de places disjoint de S_0, G vérifie l'approximation faible pour S. On abrégera ceci en disant que «G vérifie (ATF)».

On dispose également d'une notion d'approximation faible et très faible pour une k-variété X. Il faut commencer par remarquer que pour chaque ensemble de places S, on définit une application diagonale par

$$\psi_S : X(k) \longrightarrow \prod_{v \in S} X(k_v)$$

où la topologie de $X(L)$, dès que L est un corps topologique, est définie dans [Con12] et la topologie du membre de droite est donnée par la topologie produit.

Définition 4.2.

1. Si S est un ensemble de places, on dit que X *vérifie l'approximation faible pour* S si ψ_S est d'image dense.

2. On dit que X *vérifie l'approximation faible* si X vérifie l'approximation faible pour k_Ω (ou de façon équivalente pour toute ensemble fini de places). On abrégera ceci en disant que «X vérifie (AF)».

3. On dit que X *vérifie l'approximation très faible* s'il existe un ensemble fini de places en dehors duquel X vérifie l'approximation faible. On abrégera ceci en disant que «X vérifie (ATF)».

Commençons par remarquer que l'espace affine vérifie l'approximation faible:

Fait 4.3. $\mathbf{A}^1_k$ vérifie l'approximation faible

Démonstration. Ce fait est plus connu sous le nom de théorème d'Artin-Whaples dont une démonstration est donnée dans [EP05, theorem 1.1.3.]. □

Si X est une k-variété lisse, elle est réunion disjointe de ses composantes connexes, celles-ci étant irréductibles, et notons $(X_i)_{i\in I}$ la collection de ces dernières. Fixons un ensemble fini S de places et remarquons alors que si $X(k_S) \neq \emptyset$, alors X vérifie l'approximation faible pour S si et seulement s'il existe i tel que $X_i(k_S) \neq \emptyset$ et tel que pour tout $j \neq i$ on ait $X_j(k_S) = \emptyset$.

On est donc amené à vérifier les différentes questions d'approximation pour les composantes connexes de X et on ramène de la sorte l'étude au cas d'une variété lisse irréductible.

4.2 Invariance des propriétés d'approximation entre variétés irréductibles lisses stablement birationnelles

Le fait géométrique suivant est utilisé à plusieurs reprises:

Fait 4.4. Soit X une variété lisse sur k et v une place de k. Si U est un ouvert dense de X (pour la topologie de Zariski), alors $U(k_v)$ est dense dans $X(k_v)$ pour la topologie analytique.

Démonstration. Soit U comme dans l'énoncé. L'énoncé souhaité étant local sur $X(k_v)$ on peut supposer que X est affine et donc qu'il existe n et I un idéal de $k[x_1, \dots, x_n]$ tel que $X(k_v) = \mathcal{Z}_{k_v^n}(I)$ et g tel que $U(k_v) = \mathcal{D}_{k_v^n}(g)$.

Il suffit de montrer que $X(k_v) - U(k_v) = \mathcal{Z}_{k_v^n}((g) + I)$ est d'intérieur analytique vide. Supposons donc qu'il est d'intérieur non vide et soit x un élément de son intérieur. Puisque le théorème des fonctions implicites vaut sur k_v (ceci est classique pour la place à l'infini; pour les places archimédiennes, voir par exemple [Ser06, p.84, section 2.]), on dispose d'un voisinage ouvert V de x dans $X(k_v) - U(k_v)$ et d'une carte $\varphi : V \xrightarrow{\sim} W$ où W est un ouvert de k_v^d (avec $d = \dim_x X$), si bien que $g \circ \varphi^{-1} = 0$. Notons que φ^{-1} induit une immersion $k_v^d \hookrightarrow k_v^n$. Puisque $0 = d_{\varphi(x)}(g \circ \varphi^{-1}) = (d_x g) \circ \left(d_{\varphi(x)}\varphi^{-1}\right)$ on en déduit que $d_x g = 0$ si bien que la fonction polynomiale $g : k_v^n \longrightarrow k_v$ a un développement de Taylor nul en x et donc $g = 0$, ce qui est absurde. $\square$

On en déduit le résultat d'invariance suivant concernant les propriétés d'approximation:

Proposition 4.5. Soient X et Y deux variétés irréductibles lisses birationnelles et S un ensemble fini de places de k. Alors, la variété X vérifie l'approximation faible pour S si et seulement si Y vérifie l'approximation faible pour S.

Démonstration. Il suffit de traiter le cas où Y est un ouvert non vide U de X. Supposons que U vérifie l'approximation faible pour S. D'après le fait (4.4) $U(k_v)$ est dense dans $X(k_v)$ pour tout v dans S et donc $\prod_{v\in S} U(k_v)$ est dense dans $\prod_{v\in S} X(k_v)$. Ainsi, $U(k)$ est dense dans $\prod_{v\in S} X(k_v)$ et a fortiori $X(k)$ l'est aussi.

Réciproquement, supposons que X vérifie l'approximation faible pour S. Si $(x_v)_{v\in S}$ sont des points locaux de U, on sait qu'on dispose de points rationnels de X infiniment proches de $(x_v)_{v\in S}$. Mais de tels points rationnels sont forcément dans $X(k) \cap U(k_v) = U(k)$ et donc U vérifie l'approximation faible pour S. $\square$

Remarque 4.6. Si X et Y sont deux variétés sur k et S un nombre fini de places, alors $X \times_k Y$ vérifie l'approximation faible pour S si et seulement X et Y vérifient l'approximation faible pour S.

En combinant la proposition (4.5) et la remarque (4.6) au fait (4.3) on en déduit le corollaire suivant:

Corollaire 4.7. Soient X et Y deux variétés irréductibles lisses stablement birationnelles et S un nombre fini de places de k. La variété X vérifie l'approximation faible pour S si et seulement si Y vérifie l'approximation faible pour S.

En particulier, X vérifie (AF) (resp. (ATF)) si et seulement si Y vérifie (AF) (resp. (ATF)).

4.3 Caractérisation géométrique de l'approximation faible pour un groupe fini

Nous avons défini l'approximation faible pour un ensemble de place à la fois pour les groupes finis et les variétés. En réalité, l'approximation faible pour un groupe fini est équivalente à l'approximation faible pour des variétés quotients que nous définissons dans cette sous-section.

4.3.1 Le lemme sans nom: cas d'un groupe abstrait

Dans ce paragraphe, G désigne un groupe abstrait et K un corps quelconque.

Proposition 4.8 (Lemme sans nom)**.** Si V et W sont deux représentations fidèles de G sur K alors $K(V)^G$ et $K(W)^G$ sont stablement birationnellement équivalents.

Avant d'en donner une démonstration, commençons par rappeler le lemme de Speiser sans démonstration, puisqu'il a déjà fait l'objet de la proposition (3.7):

Lemme 4.9. Si L/K est une extension galoisienne de corps de groupe de Galois G et E est un K-espace vectoriel muni d'une action semi-linéaire de G, alors le morphisme canonique $L \otimes_K E^G \longrightarrow E$ est un isomorphisme.

Avec les notations du lemme de Speiser, on a:

Corollaire 4.10. L'extension $L(E)^G/K$ est transcendante pure.

Démonstration. Par le lemme de Speiser, on peut supposer que $L(E) = L(t_1, \dots, t_n)$ (où $n = \dim_K E^G$) où G agit trivialement sur les t_i. Alors $L(E)^G = K(t_1, \dots, t_n)$ est rationnelle sur K. □

On peut alors démontrer le «lemme sans nom»:

Démonstration. Soient V et W comme dans l'énoncé. On applique le corollaire (4.10) à l'extension galoisienne $K(V)/K(V)^G$ ainsi qu'au $K(V)$-espace vectoriel $E := W \otimes_K K(V)$ et on trouve donc que l'extension

$$K(V \oplus W)^G/K(V)^G$$

est rationnelle. En échangeant les rôles de V et W, on trouve également que

$$K(V \oplus W)^G/K(W)^G$$

est rationnelle et donc $K(V)^G$ et $K(W)^G$ sont stablement birationnels. □

4.3.2 Le lemme sans nom: cas d'un groupe fini étale

Nous donnons maintenant un énoncé du «lemme sans nom» qui généralise le précédent au cas d'un groupe algébrique fini sur un corps de caractéristique nulle:

Proposition 4.11. Soit G un groupe fini étale sur un corps K de caractéristique nulle et V, W des représentations fidèles de G: notons $\mathbf{A}^m_K$ et $\mathbf{A}^n_k$ des espaces affines, correspondant respectivement à V et W, sur lesquels G agit fidèlement. Alors $K(\mathbf{A}^m_K/G)$ et $K(\mathbf{A}^n_K/G)$ sont stablement birationnels.

Démonstration. Choisissons, en utilisant le fait (0.12), un ouvert X (resp. Y) de $\mathbf{A}^m_K$ (resp. $\mathbf{A}^n_K$) sur lequel G agit librement. En faisant agit G sur $X \times_K \mathbf{A}^n_K$ diagonalement, la liberté de l'action assure que le diagramme suivant est cartésien

$$\begin{tikzcd} X \times_K \mathbf{A}^n_K \arrow[r] \arrow[d] & (X \times_K \mathbf{A}^n_K)/G \arrow[d] \\ X \arrow[r] & X/G \end{tikzcd}$$

où le quotient $X \to X/G$ est fppf en vertu de (0.22). On peut donc descendre la structure de fibré vectoriel de $X \times_k \mathbf{A}^n_K \to X$ sur $(X \times_K \mathbf{A}^n_K)/G \to X/G$: celui-ci étant alors localement trivial pour la topologie fppf, il l'est également pour la topologie de Zariski en vertu de Hilbert 90 (voir [Mil80, chapter III, §4, proposition 4.9.]). En particulier, $(X \times_K \mathbf{A}^n_K)/G \to X/G$ est stablement birationnel à X/G et puisque $(X \times_K Y)/G$ est un ouvert de $(X \times_K \mathbf{A}^n_K)/G$, il suit que $(X \times_K Y)/G$ est stablement birationnel à X/G.

Le même raisonnement assure que $(X \times_K Y)/G$ est stablement birationnel à Y/G. En particulier, X/G et Y/G sont stablement birationnels, ce qui conclut. □

4.3.3 Approximation pour un groupe fini étale

Soit G un groupe fini étale sur un corps de nombres k, $\mathbf{A}^n_k$ un espace affine sur lequel G agit fidèlement, $X := \mathbf{A}^n_k/G$ la variété quotient et X^{nr} le lieu de lissité de X. Ce paragraphe est dédié au résultat suivant:

Proposition 4.12. Soit S un ensemble fini de places de k. Pour que G vérifie l'approximation faible pour S, il faut et il suffit que X^{nr} vérifie l'approximation faible pour S.

Démonstration. En vertu de (4.7) et (4.11), on peut d'emblée supposer que $X = \mathrm{GL}_n/G$ et donc que $X = X^{\text{nr}}$. Rappelons qu'une suite $(A, *) \xrightarrow{f} (B, *) \xrightarrow{g} (C, *)$ d'ensembles pointés est dite exacte si $g^{-1}(*) = f(A)$.

La suite exacte de Γ_k-ensembles pointés

$$1 \longrightarrow G(\overline{k}) \longrightarrow \mathrm{GL}_n(\overline{k}) \longrightarrow X(\overline{k}) \longrightarrow \{*\}$$

et les suites exactes de Γ_{k_v}-ensembles pointés (pour $v \in S$)

$$1 \longrightarrow G(\overline{k_v}) \longrightarrow \mathrm{GL}_n(\overline{k_v}) \longrightarrow X(\overline{k_v}) \longrightarrow \{*\}$$

induisent des suites exactes en cohomologie non abélienne (voir [Ser94, I, §5, proposition 36]) qui s'insèrent dans les lignes du diagramme commutatif suivant:

$$\begin{tikzcd} X(k) \arrow[r, "\delta"] \arrow[d, "\beta"'] & H^1(k,G) \arrow[r] \arrow[d, "\gamma"'] & H^1(k,\mathrm{GL}_n) \arrow[d] \\ \prod_{v\in S} X(k_v) \arrow[r, "\epsilon"] & \prod_{v\in S} H^1(k_v,G) \arrow[r] & \prod_{v\in S} H^1(k_v,\mathrm{GL}_n) \end{tikzcd}$$

où δ et ϵ sont des applications continues, les H^1 et $X(k)$ étant munis de la topologie discrète et les $X(k_v)$ de la topologie v-adique.

En vertu du théorème 90 de Hilbert, $H^1(K, \mathrm{GL}_n) = \{*\}$ pour tout corps K, si bien que le diagramme précédent devient:

$$\begin{tikzcd} X(k) \arrow[r, "\delta"] \arrow[d, "\beta"'] & H^1(k,G) \arrow[r] \arrow[d, "\gamma"'] & \{*\} \arrow[d] \\ \prod_{v\in S} X(k_v) \arrow[r, "\epsilon"] & \prod_{v\in S} H^1(k_v,G) \arrow[r] & \{*\} \end{tikzcd}$$

D'emblée, si β est d'image dense alors $\epsilon\beta$ est d'image dense car ϵ est continue. Puisque les H^1 sont munis de la topologie discrète, on en déduit que $\epsilon\beta$ est surjective d'où il suit que γ est surjective. Autrement dit, si X vérifie l'approximation faible pour S, alors G vérifie l'approximation faible pour S.

Réciproquement, supposons que γ est surjective. Si $(x_v)_{v\in S} \in \prod_{v\in S} X(k_v)$, on peut alors trouver $x \in X(k)$ tel que x et $(x_v)_{v\in S} \in \prod_{v\in S} X(k_v)$ s'envoient sur le même élément de $\prod_{v\in S} H^1(k_v, G)$. Or, d'après [Ser94, chapitre I, §5.4., corollaire 1], on a pour tout corps K que $H^1(K,G) = X(K)/\mathrm{GL}_n(K)$: pour toute place v de S, on peut donc trouver $y_v \in \mathrm{GL}_n(k_v)$ tel que $x_v = y_v.x$. Mais puisque GL_n est rationnelle, elle vérifie (AF) et on peut donc choisir $y \in \mathrm{GL}_n(k)$ arbitrairement proche de $(y_v)_{v\in S}$, si bien que $y.x$ est arbitrairement proche de $(x_v)_{v\in S}$. De là, si G vérifie l'approximation faible pour S, alors X vérifie l'approximation faible pour S. □

4.4 Approximation faible et problème de Grunwald

Rappelons l'énoncé du problème de Grunwald:

Problème 2. Soit G un groupe fini et S un nombre fini de places de k. Considérons, pour toute place v dans S, une extension galoisienne L^v de k_v (pour simplifier, on suppose que les L^v sont toutes incluses dans une même extension de k), de groupe H_v où $H_v \leq G$. Existe-t-il une extension galoisienne L de k, de groupe G, telle que $L_v = L^v$, pour tout v dans S?

Cette question est souvent appelée le *problème de Grunwald pour le triplet* (G, k, S).

Une reformulation du problème de Grunwald pour le triplet (G, k, S) est que l'application

$$\text{Épi}_{\text{cont}}(\Gamma_k, G) \xrightarrow{\alpha_{G,k,S}} \prod_{v\in S} \text{Hom}_{\text{cont}}(\Gamma_{k_v}, G)/\equiv$$

est surjective, où $\text{Épi}(A, B)$ désigne les épimorphismes de A dans B, et $\phi \equiv \psi$ si et seulement s'il existe $g \in G$ tel que $\phi = g\psi g^{-1}$. Pour relier le problème de Grunwald à l'approximation faible, commençons par considérer l'application

$$\text{Hom}_{\text{cont}}(\Gamma_k, G) \xrightarrow{\beta_{G,k,S}} \prod_{v\in S} \text{Hom}_{\text{cont}}(\Gamma_{k_v}, G)/\equiv .$$

Lemme 4.13. Si G est un groupe fini et k un corps de nombres, les assertions suivantes sont équivalentes:

(i) Pour tout S, $\alpha_{G,k,S}$ est surjective.

(ii) Pour tout S, $\beta_{G,k,S}$ est surjective.

Démonstration. Il s'agit de démontrer que (ii) implique (i). Considérons S un nombre fini de places de k et $\phi_v \in \text{Hom}_{\text{cont}}(\Gamma_{k_v}, G)$, pour $v \in S$. On construit S_1, disjoint de S et indexé par les éléments de G, de la façon suivante: pour $g \in G$, on choisit une place $v_g \notin S$, telle qu'on dispose d'un morphisme surjectif $\phi_g : \Gamma_{k_{v_g}} \to < g >$ (il suffit de prendre une extension cyclotomique de k_{v_g} d'ordre divisible par l'ordre de g, ce qui existe par le théorème de la progression arithmétique de Dirichlet). On considère alors l'uplet consistant en les φ_v $(v \in S)$ et les φ_{v_g} $(g \in G)$, indexé par $S \cup S_1$. Par surjectivité de $\beta_{G,k,S\cup S_1}$, il existe $\varphi \in \text{Hom}_{\text{cont}}(\Gamma_k, G)$ tel que $\beta_{G,k,S\cup S_1}$ envoie φ sur $(\varphi_v)_{v\in S} \vee (\varphi_{v_g})_{g\in G}/\equiv$.

De là, pour tout $g \in G$, il existe $\gamma \in G$ tel que $\gamma < g > \gamma^{-1} \leq \varphi(\Gamma_k) \leq G$. Il suit que $\varphi(\Gamma_k)$ rencontre toutes les classes de conjugaison de G et donc que $\varphi(\Gamma_k) = G$, ce qui conclut. □

Puisque la surjectivité de $\beta_{G,k,S}$ est équivalente à l'approximation faible de G pour S, on déduit de (4.13):

Proposition 4.14. Soit G un groupe fini et k un corps de nombres. Pour que le groupe G vérifie l'approximation faible, il faut et il suffit que pour tout ensemble fini de places S, le problème de Grunwald pour (G, k, S) admette une réponse positive.

Un premier contre-exemple au problème de Grunwald a été apporté par Xianghao Wang en 1948, sous la forme du résultat suivant:

Théorème 4.15 (Wang)**.** Si $8|n$, il n'existe pas d'extension cyclique $K/\mathbf{Q}$ de degré n telle que $K \otimes_{\mathbf{Q}} \mathbf{Q}_2$ soit une extension cyclique non ramifiée de $\mathbf{Q}_2$.

La démonstration de Wang utilisait de la théorie du corps de classes, mais nous en présentons ici une autre, donnée dans [Swa83, §5]. Commençons par un premier lemme de théorie des nombres algébriques:

Lemme 4.16. Soit L/E une extension algébrique de corps de nombres ou de corps locaux qui est cyclique avec un groupe G, d'ordre primaire n. Si $\mathfrak{p}$ est un premier de E totalement ramifié dans L tel que $\mathfrak{p} \not| n$, alors n divise $N\mathfrak{p} - 1$.

Démonstration. Puisque $\mathfrak{p}$ est totalement ramifié dans L, on peut se ramener au cas local, quitte à compléter en $\mathfrak{p}$. Si on note v la valuation de L, on déduit de la suite exacte courte

$$1 \longrightarrow U \longrightarrow L^* \longrightarrow \mathbf{Z} \xrightarrow{v} 0$$

une suite exacte

$$E^* \longrightarrow \mathbf{Z} \longrightarrow H^1(G, U)$$

et puisque $v(E^*) = n\mathbf{Z}$, on en déduit que $\mathbf{Z}/n\mathbf{Z}$ s'injecte dans $H^1(G, U)$. Considérons maintenant la suite exacte courte

$$1 \longrightarrow U_1 \longrightarrow U \longrightarrow \kappa^* \longrightarrow 1$$

où κ désigne le corps résiduel. Puisque U_1 est un pro-p groupe, où p est le premier en dessous de $\mathfrak{p}$, il vient que la multiplication par n est injective dans U_1, et donc $0 = H^1(G, U_1) \to H^1(G, U) \to H^1(G, \kappa^*)$. Il suit que $\mathbf{Z}/n\mathbf{Z}$ s'injecte dans $H^1(G, \kappa^*) = \mathrm{Hom}(G, \kappa^*) \leq \kappa^*$. Ainsi, n divise $|\kappa^*| = N\mathfrak{p} - 1$. □

Ce lemme apparaît dans la démonstration de (4.15):

Démonstration. Raisonnons par l'absurde et supposons qu'il existe une telle extension $K/\mathbf{Q}$, de groupe G. Quitte à considérer la sous-extension de K invariante par G_{imp}, on peut supposer que $n = 2^a$, avec $a \geq 3$: considérons alors $\mathbf{Q} \leq L \leq K$ telle que $[L : \mathbf{Q}] = 2$. Puisque 2 est non ramifié dans K, il en va de même dans L: il suit qu'on peut écrire L sous la forme $\mathbf{Q}(\sqrt{m})$ où $m \equiv 5 \mod 8$. Soit $p|m$ un nombre premier tel que $p \not\equiv 1 \mod 8$. Alors p est totalement ramifié dans L.

On en déduit que p est totalement ramifié dans K. En effet, notons T son groupe d'inertie dans K et T' son groupe d'inertie dans L, si bien que le morphisme $T \to T'$ est surjectif et donc $K^T \cap L \subseteq L^{T'} = \mathbf{Q}$. Mais si $K^T \neq \mathbf{Q}$, alors $L \subseteq K^T$ (car L est l'unique extension intermédiaire de degré 2 de $K/\mathbf{Q}$, par cyclicité de cette dernière) et il viendrait alors que $L \subseteq K^T \cap L \subseteq L^{T'} = \mathbf{Q}$ ce qui serait absurde. Il suit donc que $K^T = \mathbf{Q}$ et donc que p est totalement ramifié dans K.

En appliquant le lemme (4.16) à l'extension $K/\mathbf{Q}$, il suit que n divise $p - 1$ et donc que 8 divise $p - 1$, ce qui est absurde. □

On en déduit le corollaire suivant, dont la seconde partie a été annoncée dans l'introduction de la section 3:

Corollaire 4.17. Le groupe $\mathbf{Z}/8\mathbf{Z}$ ne vérifie par l'approximation faible sur $\mathbf{Q}$. En particulier, si V est une représentation fidèle de $\mathbf{Z}/8\mathbf{Z}$, alors $\mathbf{Q}(V)^{\mathbf{Z}/8\mathbf{Z}}$ n'est pas rationnel: autrement dit, le problème de Noether n'a pas toujours une réponse positive.

Démonstration. La première assertion suit de (4.15) combiné à (4.14). La seconde assertion est conséquence de (4.7) combiné à (4.12). □

4.5 L'obstruction de Brauer-Manin

4.5.1 Accouplement et obstruction de Brauer-Manin

On introduit dans cette section un ensemble intermédiaire entre les points rationnels et les points adéliques qui est voué à mesurer l'obstruction à l'approximation faible.

Dans cette section, X désigne une k-variété lisse et on note $X(k_\Omega) = \prod_v X(k_v)$. On définit un accouplement entre $X(\mathbf{A}_k)$ et $\mathrm{Br}(X)$ comme suit:

$$\begin{array}{ccc} \mathrm{Br}(X) \times X(\mathbf{A}_k) & \xrightarrow{<|>} & \mathbf{Q}/\mathbf{Z} \\ (\alpha, (P_v)) & \longmapsto & \sum_v inv_v(P_v^*(\alpha)) \end{array}$$

où $\mathbf{A}_k$ désigne l'anneau des adèles de k, l'ensemble $X(\mathbf{A}_k)$ est identifié à une partie de $\prod_v X(k_v)$ (voir [Con12, theorem 3.6.]), le morphisme $inv_v : \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z}$ est l'invariant local et $P_v^* = \mathrm{Br}(P_v)$. Il s'agit de vérifier que la somme est bien finie, ce qui constitue:

Lemme 4.18. Pour $A \in \mathrm{Br}(X)$ et $(P_v) \in X(\mathbf{A}_k)$, il n'existe qu'un nombre fini de places v telles que $P_v^*(\alpha) \neq 0$.

Démonstration. En vertu de (2.2), commençons par choisir un ensemble fini S de places de k et $\mathcal{X}$ un $\mathscr{O}_{k,S}$-schéma tels que X soit la fibre générique de $\mathcal{X}$ et tels qu'il existe $\mathcal{A} \in \mathrm{Br}(\mathcal{X})$ qui s'envoie sur $A \in \mathrm{Br}(X)$. Quitte à élargir S, on peut également supposer que $P_v \in \mathcal{X}(\mathscr{O}_v)$ pour tout v en dehors de S. Alors, $P_v^* A = P_v^* \mathcal{A}$, donc $P_v^* A$ est issu d'un élément de $\mathrm{Br}(\mathscr{O}_v)$: or, en combinant [Mil80, IV, §1, proposition 1.6] au fait que tout corps fini est C_1, on obtient que $\mathrm{Br}(\mathscr{O}_v) = 0$. Il suit que $P_v^* A$ est nul pour v en dehors de S, ce qui conclut. □

Si X' est une compactification lisse de X, on a les inclusions suivantes

$$X(k) \subseteq X(k_\Omega) \subseteq X'(k_\Omega) = X'(\mathbf{A_k})$$

où la dernière égalité suit du critère valuatif de propreté.

Définition 4.19. L'*ensemble de Brauer-Manin de* X, noté $X(k_\Omega)^{\mathrm{Br_{nr}}}$, est l'orthogonal de $\mathrm{Br}(X')$ dans $X(k_\Omega)$ pour l'accouplement entre $\mathrm{Br}(X')$ et $X'(\mathbf{A}_k)$.

Remarque 4.20. En vertu de la discussion précédant la définition (2.13), l'ensemble de Brauer-Manin de X est une partie de $X(k_\Omega)$ indépendante du choix de la compactification lisse X'.

Commençons par remarquer que les points rationnels de X sont inclus dans l'orthogonal de $\mathrm{Br}(\mathbf{A}_k)$:

Proposition 4.21. L'ensemble $X(k)$ est inclus dans l'orthogonal de $\mathrm{Br}(X)$ dans $X(\mathbf{A}_k)$.

Démonstration. Ceci résulte de la commutativité du diagramme suivant

$$\begin{tikzcd} & X(k) \arrow[r, hook] \arrow[d] & X(\mathbf{A}_k) \arrow[d] & & \\ 0 \arrow[r] & \mathrm{Br}(k) \arrow[r] & \bigoplus_v \mathrm{Br}(k_v) \arrow[r, "\bigoplus_v inv_v"] & \mathbf{Q}/\mathbf{Z} \arrow[r] & 0 \end{tikzcd}$$

où la seconde ligne est bien définie et est exacte en vertu de la théorie des corps de classes. □

Corollaire 4.22. L'ensemble $X(k)$ est inclus dans $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$.

Il s'agit maintenant de vérifier que l'ensemble de Brauer-Manin est fermé dans $X(k_\Omega)$. Commençons par remarquer que les morphismes d'évaluation sont localement constants:

Lemme 4.23. Soit K un corps, Y une K-variété et $A \in \mathrm{Br}(X)$.

(i) Si K est un corps local, alors l'application de $Y(K)$ dans $\mathrm{Br}(K)$ qui envoie x sur x^*A est localement constante.

(ii) Si $K = \mathbf{R}$, alors l'application de $Y(\mathbf{R})$ dans $\mathrm{Br}(\mathbf{R})$ qui envoie x sur x^*A est localement constante.

Démonstration. [Poo17, proposition 8.2.9.] □

On en déduit le sorite suivant:

Proposition 4.24. (i) Pour tout $A \in \mathrm{Br}(X)$, l'application $X(\mathbf{A}_k) \xrightarrow{<A|\_>} \mathbf{Q}/\mathbf{Z}$ est localement constante.

(ii) Pour tout $A \in \mathrm{Br}(X)$, l'orthogonal de A dans $X(\mathbf{A}_k)$ est ouvert et fermé dans $X(\mathbf{A}_k)$.

(iii) L'orthogonal de $\mathrm{Br}(X)$ dans $X(\mathbf{A}_k)$ est fermé dans $X(\mathbf{A}_k)$.

(iv) L'ensemble de Brauer-Manin de X est fermé dans $X(k_\Omega)$.

(v) On a $\overline{X(k)} \subseteq X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$.

Démonstration. Le point (i) se déduit en combinant (4.18) à (4.23). Le point (ii) se déduit de (i), le point (iii) de (ii) et le point (v) suit du point (iv) et de (4.21). Pour montrer (iv), il suffit de remarquer que $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$ est l'intersection de $X(k_\Omega)$ avec l'orthogonal de $\mathrm{Br}(X')$ dans $X'(\mathbf{A}_k)$, lequel est fermé par (iii). □

Définition 4.25. On dit que l'*obstruction de Brauer-Manin est la seule à l'approximation faible pour* X si $\overline{X(k)} = X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$. On abrégera ceci en disant que «X vérifie (BMO)».

4.5.2 Généralités sur l'obstruction de Brauer-Manin

On a la propriété d'invariance birationnelle suivante:

Proposition 4.26. Si X et Y sont des variétés quasi-projectives irréductibles lisses birationnelles, alors X vérifie (BMO) si et seulement si Y vérifie (BMO).

Démonstration. Il suffit de traiter le cas où Y est un ouvert U de X. En ce cas, commençons par noter que toute compactification lisse de X est une compactification lisse de U.

Si X vérifie (BMO), tout point de $U(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$ peut être approché par des points de $X(k)$. Ceux-ci étant dans les $U(k_v)$, ils sont a fortiori dans $U(k)$.

Réciproquement, supposons que U vérifie (BMO). En vertu du point (i) de (4.24) associé à (4.4), tout point de $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$ peut être approché par des points de $U(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$: ces derniers pouvant être approchés par des points de $U(k)$, ceci conclut. □

Enfin, sous une hypothèse raisonnable de finitude, la propriété (BMO) implique la propriété (ATF):

Fait 4.27. Si X est une k-variété lisse ayant un point rationnel, vérifiant (BMO) et telle que $\mathrm{Br}_{\mathrm{nr}}(X)/\mathrm{Br}(k)$ est fini, alors X vérifie (ATF).

Démonstration. Soit X' une compactification lisse de X. Considérons $x_0 \in X(k)$ et S un ensemble fini de places contenant les places de mauvaises réduction d'un ensemble de représentants (fixé) de $\mathrm{Br}(X')/\mathrm{Br}(k)$.

Montrons que X vérifie (AF) en dehors de S. Soit T un ensemble fini de places ne rencontrant pas S et $(P_v)_{v\in\Omega_k}$ une famille de points locaux de X qu'on cherche à approcher par un point rationnel de X au places de T. Posons $(Q_v)_{v\in\Omega_k}$ la famille de points locaux de X (et donc un point adélique de X') définie par $Q_v = P_v$ pour $v \notin S$ et $Q_v = x_0$ pour $v \in S$: le choix de S assure donc que $(Q_v)_{v\in\Omega_k} \in X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$. Puisque X vérifie (BMO), on peut alors approcher $(Q_v)_{v\in\Omega_k}$ par un point rationnel de X en les places de T: il en va donc de même pour $(P_v)_{v\in\Omega_k}$, ce qui conclut. □

Une première classe de groupes vérifiant (BMO) est celle des groupes abéliens:

Théorème 4.28. Les k-groupes abéliens finis vérifient (BMO).

Sans donner les détails de la démonstration, on peut montrer que si G est un k-groupe fini abélien muni d'une représentation fidèle sur un espace affine $\mathbf{A}^n_k$, alors $\mathbf{A}^n_k/G$ est stablement birationnel à un tore (voir [Vos73, theorem 1.]). Or, les tores vérifient (BMO), ce qui constitue un résultat de Sansuc et Voskresenskiĭ: pour une référence, on pourra voir [Bor96, proposition 3.3.].

4.6 Approximation hyper-faible et problème de Galois inverse

Commençons par introduire l'approximation hyper-faible pour un k-groupe fini. Pour tout ensemble fini S de places de k, rappelons qu'on note φ_S l'application $H^1(k,G) \to \prod_{v\in S} H^1(k_v,G)$.

Définition 4.29. Soit G un k-groupe fini. Si v est une place non archimédienne de k, on dit que G est non ramifié en v si le groupe d'inertie en v agit trivialement sur $G(\overline{k})$, auquel cas on note $H^1_{\mathrm{nr}}(k_v, G)$ le sous-ensemble de $H^1(k_v, G)$ qui est l'image de $H^1(\mathrm{Gal}(k_v^{\mathrm{nr}}/k_v), G(\overline{k}))$.

On dit que G *vérifie l'approximation hyper-faible* s'il existe un ensemble fini S_0 de places de k contenant la place à l'infini et les places de ramification de G, tel que pour tout ensemble fini S de places disjoint de S_0 l'image de φ_S contient $\prod_{v\in S} H^1_{\mathrm{nr}}(k_v, G)$. On abrégera ceci en disant que «G vérifie (AHF)».

On dispose alors du lien suivant entre la propriété (AHF) et le problème de Galois inverse:

Proposition 4.30. Soit G un groupe fini (abstrait). Si le groupe constant associé à G vérifie (AHF), alors G est un groupe de Galois sur k.

Démonstration. Soit S_0 un ensemble fini de places comme dans la définition (4.29). Soient $C_1, \dots, C_r$ les classes de conjugaison de G: pour tout $i \in \{1, \dots, r\}$, choisissons une place v_i de k hors de S_0 et un élément $a_i \in H^1_{\mathrm{nr}}(k_{v_i}, G) \simeq \mathrm{Hom}_{\mathrm{cont}}(\widehat{\mathbf{Z}}, G)$ d'image rencontrant C_i, les v_i étant deux à deux distincts. Puisque G vérifie (AHF), il existe par définition $a \in H^1(k, G)$ tel que pour tout i, a s'envoie sur $a_i \in H^1(k_{v_i}, G)$. Choisissons $\alpha : \Gamma_k \to G$ un représentant de a et notons H son image. Le choix des a_i assure alors que H rencontre tous les C_i et donc toutes les classes de conjugaison de G: autrement dit $H = G$. Si L est une extension galoisienne de k telle que $\ker \alpha = \mathrm{Gal}(\overline{k}/L)$, il suit alors que $G = \mathrm{Gal}(L/k)$ ce qui conclut. $\square$

5 Un lemme d'Ekedahl

Le théorème qui fait l'objet de cette section est démontré par Ekedahl dans [Eke90, lemma 1.2.] et constitue une version géométrique de l'énoncé fort du théorème de Chebotarev en théorie des nombres, où les densités sont naturelles (et non analytiques). En ajustant l'argument, on peut également obtenir un résultat faisant intervenir des densités analytiques, ce qui est fait dans [Pin97, Appendix B], mais la version qui suit est suffisante pour la suite:

Théorème 5.1. Soit R le localisé d'un anneau d'entiers d'un corps de nombres hors d'un ensemble fini de places, $\pi : \mathscr{X} \to \operatorname{Spec}(R)$ un morphisme dominant de type fini et un revêtement étale galoisien $\rho : \mathscr{Y} \to \mathscr{X}$ de groupe G tel que $\pi\rho$ est à fibre générique géométriquement irréductible.

Soit C une classe de conjugaison de G et $c = \frac{|C|}{|G|}$. Pour tout premier non nul $\mathfrak{p}$ de R, soit $t(\mathfrak{p})$ le nombre de $x \in \mathscr{X}(\kappa(\mathfrak{p}))$ tels que le Frobenius en x est dans C. Alors

$$t(\mathfrak{p})/\#\mathscr{X}(\kappa(\mathfrak{p})) - c = O\left(|\kappa(\mathfrak{p})|^{-1/2}\right).$$

Démonstration. Quitte à restreindre $\operatorname{Spec}(R)$, on peut supposer que toutes les fibres de $\pi\rho$ sont géométriquement irréductibles, de dimension $d := \dim \mathscr{Y} - \dim \mathscr{X}$ et choisir un premier l inversible sur $\mathscr{X}$. De plus, pour tout point spécial $\mathfrak{p}$ de $\operatorname{Spec}(R)$, le revêtement $\mathscr{Y}_{\mathfrak{p}} \to \mathscr{X}_{\mathfrak{p}}$ est galoisien de groupe G.

Soit χ un $\mathbf{C}$-caractère irréductible de G et ξ une $\mathbf{C}$-représentation irréductible associée. Choisissons $E \subseteq \mathbf{C}$ un corps de nombres sur lequel ξ est définie ainsi qu'un plongement $E \hookrightarrow \overline{\mathbf{Q}_l}$. Alors, ξ induit une représentation du groupe fondamental étale de $\mathscr{X}$ sur $\overline{\mathbf{Q}_l}$ et donc un $\overline{\mathbf{Q}_l}$-faisceau lisse $\mathcal{F}_l$. Il induit sur chaque fibre de X (au-dessus de $\operatorname{Spec}(R)$) un $\overline{\mathbf{Q}_l}$-faisceau lisse qu'on notera encore $\mathcal{F}_l$.

Si $x \in \mathscr{X}$ est au-dessus d'un corps fini, de Frobenius Frob_x, on a par construction $\chi(\operatorname{Frob}_x) = \operatorname{tr}\left(\operatorname{Frob}_x|_{\mathcal{F}_{l,\overline{x}}}\right)$. En posant $\mathscr{X}_{\overline{\kappa(\mathfrak{p})}} = \mathscr{X}_{\mathfrak{p}} \otimes_{\kappa(\mathfrak{p})} \overline{\kappa(\mathfrak{p})}$, la formule des traces de Grothendieck-Lefschetz (voir [Del77, Théorème 3.2.]) assure que pour tout point spécial $\mathfrak{p}$ de $\operatorname{Spec}(R)$ on a:

$$\sum_{x \in \mathscr{X}(\kappa(\mathfrak{p}))} \chi(\operatorname{Frob}_x) = \sum_{i=0}^{2d} (-1)^i \operatorname{tr}\left(\operatorname{Frob}^*, H^i_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)\right)$$

où Frob désigne le morphisme de Frobenius géométrique. De plus, puisque $\mathcal{F}_l$ est mixte de poids nul, on sait par [Del80, Théorème 3.3.1.] que les valeurs propres de Frob^* sur $H^i_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)$ sont des éléments algébriques de module complexe inférieur à $|\kappa(\mathfrak{p})|^{i/2}$.

Du fait que la dimension de $H^i_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)$ est bornée indépendamment de $\mathfrak{p}$, il suit pour $0 \leq i < 2d$ que $\operatorname{tr}\left(\operatorname{Frob}^*, H^i_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)\right) \in \mathcal{O}\left(|\kappa(\mathfrak{p})|^{d-1/2}\right)$.

Montrons maintenant que $\operatorname{tr}\left(\operatorname{Frob}^*, H^{2d}_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)\right) = \delta_{\chi,\,\text{trivial}} |\kappa(\mathfrak{p})|^d$. Commençons par remarquer que $H^{2d}_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)$ est isomorphe au dual de $H^0_{\text{ét}}(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{G}(d))$

où $\mathcal{G} = \underline{\mathrm{Hom}}(\mathcal{F}_l, \overline{\mathbf{Q}_l})$ et $\mathcal{G} = \mathcal{F}_l \otimes_{\overline{\mathbf{Q}_l}} \overline{\mathbf{Q}_l}(d)$: ceci suit de la dualité de Poincaré si $\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}$ est lisse (par passage à la limite dans [Mil80, theorem 11.1]) et de la suite exacte de la remarque [Mil80, III, 1.30.] couplée au théorème [Mil80, VI, 1.1.] dans le cas général. Fixons $\overline{s}$ un point géométrique de $\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}$. L'équivalence de catégorie entre les $\overline{\mathbf{Q}_l}$-faisceaux lisses sur $\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}$ et les $\overline{\mathbf{Q}_l}$-espaces vectoriels munis d'une action continue de $\pi_1(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \overline{s})$ (voir [FK88, appendix A, proposition 1.8]) permet d'identifier $H^0(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{G})$ au sous-espace de la fibre $\mathcal{G}(d)_{\overline{s}}$ constitué des invariants sous l'action de $\pi_1(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \overline{s})$.

Mais $\pi_1(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \overline{s})$ est un sous-groupe de $\pi_1(\mathscr{X}_{\mathfrak{p}}, \overline{s})$ et ce sous-groupe agit sur $\mathcal{G}(d)_{\overline{s}}$ à travers $\ker(G \to G'')$ où G'' est le groupe de Galois du corps des constantes de la $\kappa(\mathfrak{p})$-variété $\mathscr{Y}_{\mathfrak{p}}$: mais puisque cette dernière est géométriquement irréductible, $G'' = 1$ et donc les invariants de $\mathcal{G}(d)_{\overline{s}}$ sous $\pi_1(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \overline{s})$ correspondent aux invariants de $\mathcal{G}(d)_{\overline{s}}$ sous l'action de G. Ainsi, si χ est non trivial, $H^0_{\text{ét}}(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{G}(d))$ est nul et si χ est trivial alors $H^0_{\text{ét}}(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{G}(d))$ est égal à $\overline{\mathbf{Q}_l}(d)$. Dans ce dernier cas, $H^{2d}_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)$ est le dual de $\overline{\mathbf{Q}_l}(d)$: c'est donc $\overline{\mathbf{Q}_l}(-d)$ sur lequel le Frobenius agit par multiplication par $|\kappa(\mathfrak{p})|^d$. De là, $H^{2d}_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)$ est un espace de dimension 1 sur lequel le Frobenius agit par multiplication par $|\kappa(\mathfrak{p})|^d$ si bien que $\mathrm{tr}\left(\mathrm{Frob}^*, H^{2d}_c(\mathscr{X}_{\overline{\kappa(\mathfrak{p})}}, \mathcal{F}_l)\right) = \delta_{\chi,\ \text{trivial}} |\kappa(\mathfrak{p})|^d$.

En combinant ces constats, on obtient que:

$$\sum_{x \in \mathscr{X}(\kappa(\mathfrak{p}))} \chi(\mathrm{Frob}_x) = \delta_{\chi,\ \text{trivial}} |\kappa(\mathfrak{p})|^d + \mathcal{O}\left(|\kappa(\mathfrak{p})|^{d-1/2}\right).$$

En particulier, si χ est le caractère trivial, on obtient $\#\mathscr{X}(\kappa(\mathfrak{p})) = |\kappa(\mathfrak{p})|^d + \mathcal{O}\left(|\kappa(\mathfrak{p})|^{d-1/2}\right)$.

En outre, si φ désigne la fonction caractéristique de C, alors $\varphi = \sum_{\chi \text{ irréductible}} a_\chi \chi$ où $a_{\text{trivial}} = c$. En multipliant l'équation du paragraphe précédent par les a_χ et en sommant sous χ, on obtient donc:

$$t(\mathfrak{p}) = \sum_{\chi \text{ irréductible}} \sum_{x \in \mathscr{X}(\kappa(\mathfrak{p}))} a_\chi \chi(\mathrm{Frob}_x) = c\,|\kappa(\mathfrak{p})|^d + \mathcal{O}\left(|\kappa(\mathfrak{p})|^{d-1/2}\right).$$

En combinant ceci au fait que $\#\mathscr{X}(\kappa(\mathfrak{p})) = |\kappa(\mathfrak{p})|^d + \mathcal{O}\left(|\kappa(\mathfrak{p})|^{d-1/2}\right)$, il vient donc:

$$t(\mathfrak{p})/\#\mathscr{X}(\kappa(\mathfrak{p})) - c = O\left(|\kappa(\mathfrak{p})|^{-1/2}\right)$$

ce qui conclut.

$\square$

6 Un lemme de Harari: le lemme «formel»

6.1 Énoncé et démonstration

Le lemme suivant, souvent appelé le «lemme formel», est dû à Harari qui le démontre dans [Har94, §2]:

Théorème 6.1. [Harari] Soit k un corps de nombres et X une variété propre, lisse et géométriquement connexe sur k. Pour tout ouvert $U \subseteq X$, tout sous-groupe fini $B \subseteq \mathrm{Br}(U)$, tout sous-ensemble fini $S \subseteq \Omega_k$ et toute famille $(P_v)_{v \in \Omega_k} \in X(\mathbf{A}_k)^{\mathrm{Br}(X) \cap B}$ telle que $(P_v)_{v \in S} \in \prod_{v \in S} U(k_v)$, il existe un sous-ensemble fini $S_1 \subseteq \Omega_k$ contenant S et une famille $(Q_v)_{v \in S_1} \in \prod_{v \in S_1} U(k_v)$ tels que $Q_v = P_v$ pour $v \in S$ et $\sum_{v \in S_1} inv_v(Q_v^* \alpha) = 0$ pour tout $\alpha \in B$.

La démonstration du «lemme formel» repose sur la caractérisation suivante du groupe de Brauer d'une variété au sein du groupe de Brauer de son corps des fonctions, dont nous présentons la démonstration de [Har94] au paragraphe suivant:

Théorème 6.2. Soit k un corps de nombres et X une variété géométriquement intègre, propre et lisse, de corps des fonctions $k(X)$. Soient $\alpha \in \mathrm{Br}(k(X))$ qui n'est pas dans $\mathrm{Br}(X)$ et U un ouvert non vide de X tel que $\alpha \in \mathrm{Br}(U)$. Alors il existe une infinité de places v de k telles que la flèche $U(k_v) \to \mathrm{Br}(k_v)$ induite par α prenne une valeur non nulle.

On peut alors donner une démonstration de (6.1):

Démonstration. Soit $B^* := \mathrm{Hom}(B, \mathbf{Q}/\mathbf{Z})$ le dual de Pontryagin de B et considérons, pour $v \in \Omega_k$, la flèche $\varphi_v : U(k_v) \to B^*$ définie en envoyant un k_v-point Q sur le caractère envoyant $\alpha \in B$ sur $inv_v(Q^* \alpha)$. Posons également Γ le sous-groupe de B^* engendré par les éléments qui sont dans l'image de φ_v, pour une infinité de places v.

En combinant le fait que $B \cap \mathrm{Br}(X)$ est fini au théorème des fonctions implicites (voir (4.4)) et au caractère localement constant de l'évaluation de chaque élément de $\mathrm{Br}(X)$ en $X(k_v)$ (voir (i) de (4.24)), on peut d'emblée supposer que pour toute place v, le point P_v est dans $U(k_v)$. De plus, quitte à agrandir S, on peut également se ramener au cas où pour tout $v \notin S$, l'application φ_v est à valeur dans Γ.

Posons alors $w := \sum_{v \in S} \varphi_v(P_v) \in B^*$ et montrons que $w \in \Gamma$: ceci permet de conclure car dans ce cas, $-w \in \Gamma$ et donc il existe un ensemble fini $T \subseteq \Omega_k - S$ ainsi qu'une famille $(Q_v)_{v \in T} \in \prod_{v \in T} U(k_v)$ tels que $-w = \sum_{v \in T} \varphi_v(Q_v)$; en posant $S_1 := S \cup T$ et $Q_v = P_v$ pour $v \in S$, on obtient alors le résultat souhaité.

Pour montrer que $w \in \Gamma$, il suffit de montrer que $\Gamma^\perp \subseteq w^\perp$: en effet, ceci suit de la dualité de Pontryagin qui assure que l'accouplement $B \times B^* \to \mathbf{Q}/\mathbf{Z}$ est parfait. Or, si $A \in B$ est orthogonal à Γ, il vient que pour toute place $v \in \Omega - S$ et tout k_v-point Q de U on a $inv_v A(Q) = 0$. Il suit alors de (6.2) que A est dans $\mathrm{Br}(X)$; mais puisque $(P_v)_{v \in \Omega_k} \in X(\mathbf{A}_k)^{B \cap \mathrm{Br}(X)}$ et $\varphi_v(P_v) \in \Gamma$ (pour $v \in \Omega_k - S$), on en déduit que $A \perp w$, ce qui conclut. □

6.2 Démonstration du théorème intermédiaire

Rappelons l'énoncé du résultat qu'il reste à montrer:

Théorème 6.2. Soit k un corps de nombres et X une variété géométriquement intègre, propre et lisse, de corps des fonctions $k(X)$. Soient $\alpha \in \mathrm{Br}(k(X))$ qui n'est pas dans $\mathrm{Br}(X)$ et U un ouvert non vide de X tel que $\alpha \in \mathrm{Br}(U)$. Alors il existe une infinité de places v de k telles que la flèche $U(k_v) \to \mathrm{Br}(k_v)$ induite par α prenne une valeur non nulle.

6.2.1 Un premier résultat sur les $k(v)$-points

On commence par montrer un premier lemme arithmétique.

Lemme 6.3. Soit L/K une extension de corps de nombres et L'/L une extension cyclique. Alors, il existe une infinité de places w de L vérifiant $f(w,v) = 1$ (où v désigne la restriction de w à K) et telles que w est inerte dans L'/L.

Démonstration. Notons S l'ensemble des places w de L vérifiant $f(w,v) = 1$ et T l'ensemble des places de L inertes dans L'. On va déterminer les densité analytique $\delta(S)$ de S et $\delta(T)$ celle de T.

Commençons par montrer que $\delta(S) = 1$: en notant S' le complémentaire de S, il suffit donc de montrer que $\delta(S') = 0$. Or, en notant S'' l'ensemble des restrictions des éléments de S' à $\mathbf{Q}$, on a pour $s > 1$:

$$\frac{\sum_{w\in S'} N(w)^{-s}}{\ln(1/(s-1))} \leq \frac{[L:\mathbf{Q}]\sum_{p\in S''} p^{-2s}}{\ln(1/(s-1))}$$

laquelle inégalité suit du fait que pour $w \in S'$ il vient, en notant $p \in \mathbf{Z}$ le premier sous w, que $f(w,p) \geq 2$ et qu'il y a au plus $[L:\mathbf{Q}]$ places de K au-dessus de p. Puisque le terme droite tend vers 0 lorsque s tend vers 1^+, on en déduit que $\delta(S') = 0$.

Montrons ensuite que $\delta(T) = \frac{\varphi(m)}{m}$, où $m = [L':L]$. Une place w de L étant inerte dans L' si et seulement si son groupe de Galois résiduel est d'ordre m, l'ensemble T est donc l'ensemble des places L en lequel le Frobenius est un générateur de $\mathrm{Gal}(L'/L)$. Puisqu'il y a $\varphi(m)$ générateurs de $\mathrm{Gal}(L'/L)$ (chacun formant une classe de conjugaison car l'extension est abélienne), il suit alors du théorème de Chebotarev que la densité analytique de T est égale à $\varphi(m)/m$.

Puisque $T \cup S$ contient S et que S est de densité analytique 1, on en déduit que $T \cup S$ est de densité analytique 1 et donc que $T \cap S$ a une densité analytique égale à $\delta(T \cap S) = \frac{\varphi(m)}{m}$. Mais puisque $T \cap S$ est l'ensemble considéré dans l'énoncé et qu'il est de densité analytique non nulle, on en déduit qu'il est infini. □

Il s'agit maintenant de démontrer le résultat suivant sur les $k(v)$-points:

Proposition 6.4. Soient k un corps de nombres, $\mathscr{W}$ un ouvert non vide de $\mathrm{Spec}(\mathscr{O}_k)$ et $\pi : \mathscr{X} \to \mathscr{W}$ un morphisme dominant de type fini dont la fibre générique, notée X, est supposée intègre. Soit $\rho : \mathscr{Y} \to \mathscr{X}$ un revêtement étale, connexe, cyclique de degré $m \geq 2$ de $\mathscr{X}$. Pour presque toute place v de k on dispose de $\mathscr{Y}_v$ et $\mathscr{X}_v$, les fibres respectives de $\pi\rho$ et de π au-dessus de v.

Alors il existe un ouvert $\mathscr{U}^1$ de $\mathscr{X}$ ainsi qu'un ensemble infini I de places v de k tels qu'on ait, en notant $\mathscr{U}^2 = \rho^{-1}(\mathscr{U}^1)$:

1. Pour toute place v de I, le revêtement étale $\rho(v) : \mathscr{U}^2_v \to \mathscr{U}^1_v$ est connexe.
2. Si Ω est un ouvert non vide de $\mathscr{U}^1$, sa réduction Ω_v au dessus de v admet, pour presque toute place v de I, un $k(v)$-point $P(v)$ vérifiant: la fibre de $\rho(v)$ en $P(v)$ est connexe.

Démonstration. Notons Y la fibre générique de $\pi\rho$, K le corps des fonctions de X et K' celui de Y. Posons L la clôture algébrique de k dans K et L' celle de K dans K', si bien que L'/L est une extension cyclique d'ordre s divisant m (car $[L' : L] = [KL' : K]$, lequel divise $[K' : K]$).

En utilisant le lemme (6.3), choisissons un ensemble infini I de places v de k qui soient non ramifiées dans la clôture galoisienne de L'/k telles qu'il existe au-dessus une place w de L qui est inerte dans L' et vérifie $k(v) = L(w)$.

On commence par se ramener au cas où X est géométriquement intègre sur k. Il existe un ouvert non vide U^1 de X tel que la flèche $U^1 \to \mathrm{Spec}(k)$ se factorise en $U^1 \to \mathrm{Spec}(L)$, si bien que U^1 est une L-variété géométriquement intègre: il suit qu'il existe un ouvert $\mathscr{U}^1$ de $\mathscr{X}$ tel que la flèche $\mathscr{U}^1 \to \mathscr{W}$ se factorise par une flèche $\mathscr{U}^1 \to \mathscr{W}_L$ (où $\mathscr{W}_L$ est un ouvert non vide de $\mathrm{Spec}\,\mathscr{O}_L$) de fibre générique $U^1 \to \mathrm{Spec}(L)$. Posons $\mathscr{U}^2 = \rho^{-1}(\mathscr{U}^1)$. Pour v dans I, il existe une place w de L (au-dessus de v) telle que $L(w) = k(v)$. Quitte à remplacer $\mathscr{W}$ par $\mathscr{W}_L$, $\mathscr{X}$ par $\mathscr{U}^1$ et $\mathscr{Y}$ par $\mathscr{U}^2$, on peut alors supposer que $k = L$ et donc que X est une k-variété géométriquement intègre.

On montre ensuite que ρ se factorise en un revêtement étale $\rho' : \mathscr{U}' \to \mathscr{U}^1$ où $\mathscr{U}^2 \to \mathscr{U}'$ est de fibre générique géométriquement intègre.

Soit $\mathscr{W}'$ l'image réciproque de $\mathscr{W}$ par le morphisme $\mathrm{Spec}(\mathscr{O}_{L'}) \to \mathrm{Spec}(\mathscr{O}_k)$ et posons $\mathscr{U}' = \mathscr{U}^1 \times_{\mathscr{W}} \mathscr{W}'$. Par définition de L', on peut alors supposer que le revêtement $\mathscr{U}^2 \to \mathscr{U}^1$ se factorise par le revêtement étale connexe $\rho' : \mathscr{U}' \to \mathscr{U}_1$. Comme $\mathscr{U}^2 \to \mathscr{U}'$ est de fibre générique géométriquement intègre, il suit que $\rho(v)$ est connexe pour presque toute place de I.

On montre enfin que ρ se factorise également en un revêtement étale $\rho'' : \mathscr{U}'' \to \mathscr{U}^1$ de fibre générique géométriquement intègre.

Soit $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ ($\alpha_i \geq 1$) la décomposition de m en nombres premiers et supposons que $p_1, \dots, p_r$ ($r \leq s$) sont les p_i ne divisant par $t = [L' : k]$. Il existe alors une unique extension K''/K intermédiaire de K'/K telle que K''/K est de degré $t' = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Puisque t et t' sont premiers entre eux, on a $K'' \cap KL' = K$, d'où on déduit que k est algébriquement clos dans K''. Quitte à réduire les $\mathscr{U}^i$, il suit qu'on peut factoriser $\mathscr{U}^2 \to \mathscr{U}^1$ par un revêtement étale connexe $\mathscr{U}^2 \to \mathscr{U}''$, où $\rho'' : \mathscr{U}'' \to \mathscr{U}^1$ a pour fibre générique K'', d'où il suit que cette dernière est géométriquement intègre.

Considérons Ω un ouvert de $\mathscr{U}^1$. En appliquant le lemme d'Ekedahl (5.1) à $\rho'' \times_{\mathscr{U}^1} \Omega$ on obtient, pour presque toute place v de I, un point $P(v)$ de $\Omega(k(v))$ en lequel le Frobenius engendre $\mathrm{Gal}(\rho'')$ et en lequel la fibre de $\rho''(v)$ est connexe. En outre, pour tout $v \in I$, puisque v est inerte dans l'extension L'/k, toutes les fibres de $\rho'(v)$ sont connexes: en particulier, la fibre de $\rho'(v)$ en $P(v)$ est connexe. On en déduit que la fibre de $\rho(v)$ en $P(v)$ est également connexe: en effet, si $F \in \mathrm{Gal}(K'/K)$ désigne le Frobenius en $P(v)$, il engendre $\mathrm{Gal}(K''/K)$ (resp. $\mathrm{Gal}(KL'/K)$) car la fibre de $\rho''(v)$ (resp. $\rho'(v)$) est connexe en $P(v)$. Or, du fait que $KL' \cap K'' = K$, on déduit une injection

$$\mathrm{Gal}(K'/K) \hookrightarrow \mathrm{Gal}(KL'/K) \times \mathrm{Gal}(K''/K)$$

et donc $m \leq t.t' \leq m$ d'où il vient que ce morphisme est bijectif: en utilisant que F engendre $\mathrm{Gal}(KL'/K)$ et $\mathrm{Gal}(K''/K)$, on en conclut que F engendre $\mathrm{Gal}(K'/K)$, et donc que la fibre de $\rho(v)$ en $P(v)$ est connexe. □

6.2.2 Calcul des $\alpha(P_v)$

Commençons par remarquer le fait suivant, qui assure que l'énoncé de (6.2) est local:

Fait 6.5. Soit X une k-variété géométriquement intègre, propre, lisse et α un élément de n-torsion de $\mathrm{Br}(k(X))$ qui se trouve hors de $\mathrm{Br}(X)$. Alors, il existe un modèle complet lisse $\mathscr{X}$ de X au-dessus d'un ouvert non vide $\mathscr{W} = \mathrm{Spec}(\mathscr{O}_{k,S})$ de $\mathrm{Spec}(\mathscr{O}_k)$, un ouvert affine non vide $\mathscr{V}$ de $\mathscr{X}$ et un fermé $\mathscr{B}$ intègre de codimension 1 de $\mathscr{V}$, lisses au-dessus de $\mathscr{W}$ vérifiant:

1. En posant $\mathscr{U} = \mathscr{V} - \mathscr{B}$, on a $\alpha \in \mathrm{Br}(\mathscr{U})$.
2. Le résidu de α au point générique de $\mathscr{B}$ est un élément non nul de $H^1_{\text{ét}}(\mathscr{B}, \mathbf{Z}/n\mathbf{Z})$.
3. L'entier n est premier aux caractéristiques résiduelles de $\mathscr{W}$.

Démonstration. Choisissons $\mathscr{X}$ un modèle propre lisse de X au-dessus d'un ouvert $\mathscr{W} = \mathrm{Spec}(\mathscr{O}_{k,S})$ de $\mathrm{Spec}(\mathscr{O}_k)$ telle qu'il existe un ouvert $\mathscr{U}$ de $\mathscr{X}$ vérifiant $\alpha \in \mathrm{Br}(\mathscr{U})$. Quitte à élargir S, on peut d'emblée supposer que n est premier aux caractéristiques résiduelles de $\mathscr{W}$.

De plus, puisque $\alpha \notin \mathrm{Br}\,\mathscr{X}$, le théorème de pureté de Grothendieck fournit un point x de codimension 1 de $\mathscr{X}$ qui engendre un sous-schéma intègre lisse $\mathscr{B}'$ tel que le résidu $\mathscr{I}$ de alpha en x dans $H^1(\kappa(x), \mathbf{Q}/\mathbf{Z})$ est non nul. Il existe alors un voisinage $\mathscr{B}$ de x dans $\mathscr{B}'$ tel que $\mathscr{I} \in H^1_{\text{ét}}(\mathscr{B}, \mathbf{Q}/\mathbf{Z})$. On prend alors $\mathscr{V}$ égal à $\mathscr{U} \cup \mathscr{B}$. Quitte à restreindre $\mathscr{V}$ à un ouvert au voisinage du point générique de $\mathscr{B}$, on peut également supposer que $\mathscr{V}$ est affine. Ce choix de $\mathscr{V}$ et de $\mathscr{B}$ répond alors aux conditions de l'énoncé. □

Dans la suite, si $\mathscr{V} = \mathrm{Spec}(R)$ et $\mathscr{B} = \mathrm{Spec}(R/t)$ (avec $t \in R$) désignent des $\mathscr{W}$-schémas, où $\mathscr{W} = \mathrm{Spec}(\mathscr{O}_{k,S})$ est un ouvert non vide de $\mathscr{O}_k$, si v est une place de k en dehors de S, alors on dit d'une flèche $s : \mathrm{Spec}(\mathscr{O}_v) \to \mathscr{V}$ que c'est une section si la composition avec le morphisme structurel $\mathscr{V} \to \mathscr{W}$ est le morphisme naturel $\mathrm{Spec}(\mathscr{O}_v) \to \mathscr{W}$. L'homomorphisme $\theta : R \to \mathscr{O}_v$ associé à s envoie t sur un élément t' de $\mathscr{O}_v$ dont la valuation e est appelée la $\mathscr{B}$-multiplicité de s.

On note également $\delta_v : \mathrm{Br}(k_v) \to H^1(k(v), \mathbf{Q}/\mathbf{Z})$ et $\partial_t : \mathrm{Br}(K) \to H^1(\kappa, \mathbf{Q}/\mathbf{Z})$ les morphismes de résidu. On dispose alors du résultat suivant:

Proposition 6.6. Soient $\mathscr{W} = \mathrm{Spec}(\mathscr{O}_{k,S})$ un ouvert non vide de $\mathrm{Spec}(\mathscr{O}_k)$, $\mathscr{V} = \mathrm{Spec}(R)$ un $\mathscr{W}$-schéma intègre, régulier et $\mathscr{B} = \mathrm{Spec}(R/t)$ un sous-schéma fermé de $\mathscr{V}$ qui est intègre, régulier et de codimension 1. Soient K et κ les corps de fonctions respectifs de $\mathscr{V}$ et $\mathscr{B}$ qu'on suppose de caractéristique nulle.

Soit α un élément de n-torsion de $\mathrm{Br}(R\,[t^{-1}]) \subseteq \mathrm{Br}(K)$ dont le résidu $\chi_t := \partial_t(\alpha)$ est dans $H^1_{\text{ét}}(R/t, \mathbf{Q}/\mathbf{Z})$. Supposons également que les caractéristiques résiduelles de $\mathscr{V}$ et $\mathscr{W}$ sont premières à n. Alors, il existe un ouvert ω de $\mathscr{V}$ rencontrant $\mathscr{B}$, tel que pour toute section $s : \mathrm{Spec}(\mathscr{O}_v) \to \omega \subseteq \mathscr{V}$, de $\mathscr{B}$-multiplicité $e > 0$ finie et induisant des morphismes $s_1 : \mathrm{Spec}(k_v) \to \mathrm{Spec}(R\,[t^{-1}])$ et $s_2 : \mathrm{Spec}(k(v)) \to \mathrm{Spec}(R/t)$, on ait:

$$\delta_v(s_1^*(\alpha)) = e s_2^*(\chi_t)$$

où $s_1^* : \mathrm{Br}(R\,[t^{-1}]) \to \mathrm{Br}(k_v)$ et $s_2^* : H^1_{\text{ét}}(R/t, \mathbf{Q}/\mathbf{Z}) \to H^1(k(v), \mathbf{Q}/\mathbf{Z})$ sont associées à s_1 et s_2.

Démonstration. Commençons par montrer qu'on peut se ramener au cas où R est (t)-complet. Supposons donc le cas complet traité, notons $\widehat{R}$ la (t)-complétion de R et choisissons $\widehat{\omega}$ un ouvert comme dans l'énoncé, pour $\widehat{\mathscr{V}} = \mathrm{Spec}(\widehat{R})$, d'intersection non vide avec $\widehat{\mathscr{B}} = \mathrm{Spec}(\widehat{R}/(t))$. Puisque l'image de $\widehat{\omega}$ par $p : \mathrm{Spec}(\widehat{R}) \to \mathrm{Spec}(R)$ est pro-constructible (voir [Gro67, proposition 1.9.3]) et ne rencontre pas le point générique, elle contient un ouvert ω qui rencontre $\mathscr{B}$. En outre, toute section s : $\mathrm{Spec}(\mathscr{O}_v) \to \mathrm{Spec}(R)$ se factorise par une section $\mathrm{Spec}(\mathscr{O}_v) \to \mathrm{Spec}(\widehat{R})$ (car $\mathscr{O}_v$ est complet) de même multiplicité: pour obtenir l'égalité de l'énoncé, il reste donc à vérifier qu'il revient au même de prendre le résidu dans $H^1(\kappa, \mathbf{Q}/\mathbf{Z})$ d'un élément de $\mathrm{Br}(R\,[t^{-1}])$ d'ordre premier aux caractéristiques résiduelles, ou de prendre son image dans $\mathrm{Br}(\widehat{R}\,[t^{-1}]) \subseteq \mathrm{Br}(K)$ puis son résidu dans $H^1(\kappa, \mathbf{Q}/\mathbf{Z})$. Or, le diagramme suivant est commutatif

$$\begin{tikzcd}
\mathrm{Br}(R\,[t^{-1}]) \arrow[r] \arrow[d] & \mathrm{Br}(R_{(t)}\,[t^{-1}]) \arrow[r] \arrow[d] & H^1(\kappa, \mathbf{Q}/\mathbf{Z}) \arrow[d, "id"] \\
\mathrm{Br}(\widehat{R}\,[t^{-1}]) \arrow[r] & \mathrm{Br}((\widehat{R}_{(t)})\,[t^{-1}]) \arrow[r] & H^1(\kappa, \mathbf{Q}/\mathbf{Z})
\end{tikzcd}$$

où les flèches verticales non précisées sont issues des morphismes de complétion: en effet, le carré de gauche est commutatif par définition et celui de droite l'est en vertu de la discussion suivant [CTO89, proposition 1.1.].

Supposons donc que R est (t)-complet. Cette hypothèse permet de relever χ_t en un élément χ de $H^1_{\text{ét}}(R, \mathbf{Z}/n\mathbf{Z})$ (voir [Gab94, Theorem 1]). Considérons alors le cup-produit $\beta = \chi \smile t$ où χ est identifié à son image dans $H^1_{\text{ét}}(R\,[t^{-1}], \mathbf{Z}/n\mathbf{Z})$ et t est identifié à sa classe dans $R\,[t^{-1}]^* / (R\,[t^{-1}]^*)^n \subseteq H^1_{\text{ét}}(R\,[t^{-1}], \mathbf{Z}/n\mathbf{Z})$ (cette inclusion étant donnée par la suite de Kummer), si bien que $\beta \in H^2_{\text{ét}}(R\,[t^{-1}], \mathbf{Z}/n\mathbf{Z})$.

Il suit alors de [CTO89, proposition 1.3.] que $\partial_t(\beta) = \chi_t$: on en déduit que $\partial_t(\beta - \alpha) = 0$ et donc, par (2.5), que $\beta - \alpha$ est dans $\mathrm{Br}(R_{(t)})$. Il suit qu'il existe un ouvert ω de $\mathscr{V}$ contenant le point générique de $\mathscr{B}$ et tel que $\beta - \alpha \in \mathrm{Br}(\omega)$. Alors, si $s : \mathrm{Spec}(\mathscr{O}_v) \to \omega \subseteq \mathscr{V}$ est une section, on a $s_1^*(\beta - \alpha) \in \mathrm{Br}(\mathscr{O}_v)$ et donc $\delta_v(s_1^*(\beta - \alpha)) = 0$. Pour montrer l'égalité souhaitée, on peut donc remplacer α par β.

Or, $s_1^*(\beta) = \chi_1 \smile t'$ où $\chi_1 := s_1^*(\chi)$ est l'image de χ par $H^1_{\text{ét}}(R, \mathbf{Z}/n\mathbf{Z}) \to H^1(k_v, \mathbf{Z}/n\mathbf{Z})$ et $t' := s_1^*(t)$ est l'image de t dans $H^1(k_v, \mathbf{Z}/n\mathbf{Z})$. Il suit alors de [CTO89, proposition 1.3] que $\delta_v(s_1^*(\beta)) = e\chi_2$ où e est la multiplicité de s et χ_2 est l'image de χ dans $H^1(k(v), \mathbf{Z}/n\mathbf{Z})$ et donc $\chi_2 = s_2^*(\chi_t)$. On trouve finalement que $\delta_v(s_1^*(\beta)) = es_2^*(\chi_t)$, ce qui conclut. □

On obtient donc le calcul suivant des $\alpha(P_v)$:

Corollaire 6.7. Soient X une k-variété géométriquement intègre, α un élément de n-torsion de $\mathrm{Br}(k(X))$ et $\mathscr{X}$ un modèle de X au-dessus d'un ouvert non vide $\mathscr{W} = \mathrm{Spec}(\mathscr{O}_{k,S})$ de $\mathrm{Spec}(\mathscr{O}_k)$ où n est premier aux caractéristiques résiduelles de $\mathscr{W}$. Soient $\mathscr{V}$ un ouvert affine non vide lisse de $\mathscr{X}$ et $\mathscr{B}$ un fermé intègre et lisse de codimension 1 de $\mathscr{V}$. Supposons que le résidu $\mathscr{I}$ de α au point générique de $\mathscr{B}$ est dans $H^1_{\text{ét}}(\mathscr{B}, \mathbf{Z}/n\mathbf{Z})$ et que $\alpha \in \mathrm{Br}(\mathscr{U})$, où $\mathscr{U} = \mathscr{V} - \mathscr{B}$.

Alors, il existe un ouvert ω de $\mathscr{V}$ rencontrant $\mathscr{B}$ tel que pour tout point P_v de $\mathscr{U}(k_v)$ associé à une section $s : \mathrm{Spec}(\mathscr{O}_v) \to \omega \subseteq \mathscr{V}$ de $\mathscr{B}$-multiplicité finie $e > 0$, on ait, en notant $P(v)$ le $k(v)$-point de $\mathscr{V}$ associé à s:

1. Si $P(v) \notin \mathscr{B}(k(v))$, alors $\delta_v(\alpha(P_v)) = 0$.

2. Si $P(v) \in \mathscr{B}(k(v))$, alors
$$\delta_v(\alpha(P_v)) = e\partial$$
où ∂ est l'image de $\mathscr{I}$ via le morphisme $H^1_{\text{ét}}(\mathscr{B}, \mathbf{Z}/n\mathbf{Z}) \xrightarrow{P(v)^*} H^1(k(v), \mathbf{Z}/n\mathbf{Z})$.

Démonstration. Si $P(v) \notin \mathscr{B}(k(v))$, alors la section s est à valeur dans $\mathscr{U}$: de là, $P_v^*(\alpha)$ est dans $\mathrm{Br}(\mathscr{O}_v)$ et donc $\delta_v(\alpha(P_v)) = 0$. Si $P(v)$ est dans $\mathscr{B}$, les hypothèses de la proposition (6.6) sont vérifiées: en effet, la seule hypothèse à vérifier est que n est premier aux caractéristiques résiduelles de $\mathscr{V}$, ce qui résulte de l'hypothèse sur les caractéristiques résiduelles de $\mathscr{W}$. Dans ce cas, on dipose d'un ouvert ω de $\mathscr{V}$ rencontrant $\mathscr{B}$ et on a bien $\delta_v(\alpha(P_v)) = e\partial$ en remarquant que $s_1 : \mathrm{Spec}(k_v) \to \mathscr{U}$ et $s_2 : \mathrm{Spec}(k(v)) \to \mathscr{B}$ correspondent respectivement au k_v-point P_v et au $k(v)$-point $P(v)$. □

6.2.3 Démonstration

On peut maintenant donner une démonstration du théorème (6.2):

Démonstration. Soit k un corps de nombres, X une k-variété géométriquement intègre, propre et lisse de corps des fonctions $k(X)$. Soit $\alpha \in \mathrm{Br}(k(X))$ un élément de n-torsion en dehors de $\mathrm{Br}(X)$. En vertu du fait (6.5), on dispose d'un ouvert non vide $\mathscr{W} = \mathrm{Spec}(\mathscr{O}_{k,S})$ de $\mathrm{Spec}(\mathscr{O}_k)$ où n est inversible, d'un $\mathscr{W}$-schéma affine lisse $\mathscr{V}$ et d'un sous-schéma fermé intègre et lisse $\mathscr{B}$ de codimension 1 de $\mathscr{V}$, tel que

$\alpha \in \mathrm{Br}(\mathscr{U})$ (où $\mathscr{U} = \mathscr{V} - \mathscr{B}$). Le même fait assure qu'on peut supposer que le résidu de α au point générique de $\mathscr{B}$, noté $\mathscr{I}$, est un élément non nul de $H^1_{\text{ét}}(\mathscr{B}, \mathbf{Z}/n\mathbf{Z})$. Les hypothèses du corollaire (6.7) sont donc vérifiées et quitte à réduire $\mathscr{V}$, on peut supposer que $\omega = \mathscr{V}$.

Il suffit alors de trouver une place $v \notin S$ et un $k(v)$-point $P(v)$ de $\mathscr{B}$ qui envoie $\mathscr{I} \in H^1_{\text{ét}}(\mathscr{B}, \mathbf{Z}/n\mathbf{Z})$ sur un élément non nul ∂ de $H^1(k(v), \mathbf{Z}/n\mathbf{Z})$, puis de le relever en un $\mathscr{O}_v$-point de $\mathscr{V}$ de multiplicité 1: en effet, le corollaire (6.7) assure alors que $\delta_v(\alpha(P_v)) = \partial$ est non nul, ce qui conclut.

Commençons par trouver une telle place v et un tel $k(v)$-point. Considérons J l'image de $\mathscr{I}$ dans $H^1(\kappa, \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}_{\text{cont}}(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbf{Q}/\mathbf{Z})$ ainsi qu'une extension cyclique non triviale κ'/κ telle que J engendre $\mathrm{Hom}(\mathrm{Gal}(\kappa'/\kappa), \mathbf{Q}/\mathbf{Z})$. On dispose alors d'un ouvert non vide Ω de $\mathscr{B}$ et d'un revêtement étale cyclique connexe $\mathscr{Y} \to \Omega$ de fibre générique $\mathrm{Spec}(\kappa') \to \mathrm{Spec}(\kappa)$ et d'ordre $m \geq 2$ (avec $m = [\kappa' : \kappa]$). Dans ce cas, la fibre générique de $\mathscr{Y}$ est une k-variété intègre et les hypothèses de la propriété (6.4) sont donc vérifiées, ce qui assure l'existence d'un ensemble infini I de places comme dans (6.4). Alors, pour toute place v de I on peut trouver un $k(v)$-point lisse $P(v)$ dans Ω tel que la fibre du revêtement $\mathscr{Y} \to \Omega$ en $P(v)$ est connexe. Ainsi, la fibre $\partial \in H^1(k(b), \mathbf{Q}/\mathbf{Z})$ de $\mathscr{I}$ en $P(v)$ est d'ordre $m \geq 2$ donc $\partial \neq 0$.

Relevons enfin $P(v)$ en un k_v-point de $\mathscr{V}$ de multiplicité 1. Notons π_v une uniformisante de $\mathscr{O}_v$ et posons $\mathscr{B}'_v = \mathrm{Spec}(R'/(t - \pi_v))$ où $R' = R \otimes_{\mathscr{O}_{k,S}} \mathscr{O}_v$. Alors, la fibre de $\mathscr{B}$ au-dessus de v et la fibre générique du $\mathscr{O}_v$-schéma $\mathscr{B}'_v$ sont isomorphes. Or, par le lemme de Hensel on peut relever le $k(v)$-point $P(v)$ en un $\mathscr{O}_v$-point de $\mathscr{B}'_v$, lequel correspond à un $\mathscr{O}_v$-point s de $\mathscr{V}$. De plus, s est de multiplicité 1 car $s^\# : R \to \mathscr{O}_v$ se décompose en $R \to R'/(t - \pi_v) \to \mathscr{O}_v$, si bien que t s'envoie sur π_v et donc $v(s^\#(t)) = 1$. $\square$

7 Résultat principal de l'article

Dans cette section, k désigne un corps de nombres. Le résultat que nous présentons est le théorème 1 de [Har07]:

Théorème 7.1. Soit

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

une extension scindée de k-groupes finis, avec A abélien. Si G vérifie (BMO), alors il en va de même pour E.

7.1 Un premier résultat sur les variétés fibrées

Cette section est dédiée à un lemme de transfert de la propriété (BMO) «en famille». Commençons par rappeler la notion d'ensemble hilbertien, dont une étude approfondie est proposée dans [Ser08]:

Définition 7.2. Si V est une k-variété intègre, un sous-ensemble H de $V(k)$ est dit *hilbertien élémentaire* s'il existe un ouvert de Zariski non vide de V et un revêtement étale $\rho : U' \to U$ où U' est intègre et H est l'ensemble des k-points de U en lesquels la fibre de ρ est connexe.

On dit que H est *hilbertien* s'il est intersection finie de sous-ensembles hilbertiens élémentaires.

Pour le lemme qui suit, on a besoin du fait suivant:

Fait 7.3. L'intersection de deux sous-ensemble hilbertiens non vides d'une variété intègre contient un sous-ensemble hilbertien élémentaire non vide.

Démonstration. [Lan83, propositions 5.1. et 5.2.] □

On dispose alors du lemme suivant:

Lemme 7.4. Soit B une k-variété lisse et géométriquement intègre telle que $B(k_\Omega) \neq \emptyset$ et vérifiant l'approximation faible en dehors d'un ensemble fini S_0 de places.

Soit S un ensemble fini de places et $(P_v)_{v\in S}$ des points locaux de B vérifiant: pour tout ensemble fini S_1 de places disjoint de $S \cup S_0$ et toute famille $(M_v)_{v\in S_1}$, la famille obtenue en adjoignant celle des (P_v) à celle des (M_v) est dans l'adhérence de $B(k)$, pour la topologie produit.

Alors, si H est un sous-ensemble hilbertien de $B(k)$, il existe un point de H arbitrairement proche des P_v $(v \in S)$.

Démonstration. Soient S_0, S et $(P_v)_{v\in S}$ comme dans l'énoncé. Considérons H un sous-ensemble hilbertien de $B(k)$ et $\rho : U' \to U$ un revêtement étale, où U est un ouvert de B, la variété U' est intègre, et tel que H contient l'ensemble des k-points de U dont la fibre est connexe (l'existence d'un tel revêtement suit de (7.3)).

Quitte à prendre une clôture normale L de $k(U')/k(U)$, à étendre l'extension $L/k(U)$ en un revêtement étale d'un ouvert de U et quitte à réduire U, on est ramené à traiter le cas où $\rho : U' \to U$ est un revêtement galoisien de groupe J. Notons

k' la clôture algébrique de k dans $k(U')$, si bien que, quitte à réduire U', on peut voir U' comme une k'-variété (car ρ étant étale et U normale, U' est normale), d'où il suit que $U' \to U \otimes_k k'$ est un revêtement étale galoisien au dessus de k' (de groupe $J_0 \trianglelefteq J$), avec U' qui est une k'-variété géométriquement intègre (pour ce dernier point, voir par exemple [Liu02, chapter 3, remark 2.9.]). En posant ensuite $U'' := U \otimes_k k'$, on peut étendre le diagramme commutatif de k-schémas

$$\begin{tikzcd} & U' \arrow[dl, "\rho"'] \arrow[dr, "\rho'"] & \\ U & & U'' \arrow[ll] \end{tikzcd}$$

en un diagramme

$$\begin{tikzcd} & \mathcal{U}' \arrow[dl] \arrow[dr] & \\ \mathcal{U} & & \mathcal{U}'' \arrow[ll] \end{tikzcd}$$

au-dessus d'un ouvert de $\operatorname{Spec}(\mathscr{O}_k)$ contenant $\operatorname{Spec}(\mathscr{O}_{k,S_0})$ où les flèches diagonales sont des revêtements étales galoisiens.

D'après le théorème de Chebotarev, il existe une infinité de places de k qui sont totalement décomposées dans k' et donc il y a un ensemble infini I de places w de k' telles que $k'(w) = k(v)$ (où v est la restriction de w à k). De plus, puisque $\mathcal{U}' \to \mathcal{U}''$ est un revêtement étale galoisien au-dessus de k' à fibre générique géométriquement intègre, le lemme d'Ekedahl (5.1) assure que presque toute place w de k' vérifie: pour toute classe de conjugaison c de J, il existe un $k'(w)$-point de U'' dont le Frobenius appartient à c. Mais puisque I est infini on peut même choisir w dans une partie cofinie de I, si bien que $k'(w) = k(v)$ et donc ce $k'(w)$-point de U'' correspond à un $k(v)$-point $\widetilde{M_v}$ de U qu'on peut, par le lemme de Hensel, relever en un k_v-point M_v de U.

On peut donc choisir, pour chaque classe de conjugaison c de J, une place v de k en dehors de $S \cup S_0$ et un k_v-point M_v de U dont le Frobenius du réduit modulo v est dans c: notons S_1 cet ensemble de places. Par hypothèse, il existe un point rationnel $m \in U(k)$ arbitrairement proche des M_v ($v \in S_1$) et des P_v ($v \in S$).

Or, la fibre de ρ en m est connexe car le groupe de décomposition de J en m est égal à J: en effet, si c est une classe de conjugaison de J, il existe une place v de S_1 telle que le Frobenius du réduit de m modulo v est dans c (car m est proche de M_v et ceci est vérifié pour M_v); on en déduit que le groupe de décomposition de m rencontre toutes les classes de conjugaison de J et donc égale J. De la sorte, m est un point de H arbitrairement proche des P_v, ce qui conclut. □

Remarque 7.5. Dans la suite, le lemme est utilisé sous la forme qui suit. Supposons que B vérifie (BMO) et que $\operatorname{Br}_{\mathrm{nr}}(B)/\operatorname{Br}(k)$ est fini. Considérons $E \subseteq \operatorname{Br}_{\mathrm{nr}}(B)$ un ensemble de représentants du quotient et prenons S_0 un ensemble fini de places contenant les places de mauvaise réduction de E et tel que B vérifie (AF) en dehors de S_0.

Sous ces conditions, l'hypothèse est vérifiée pour tout ensemble fini S de places et toute famille $(P_v)_{v \in S}$ de points locaux qui est la projection d'un élément de $X(k_\Omega)^{\operatorname{Br}_{\mathrm{nr}}}$: en effet, si $v \notin S_0$ et M_v est un point local, alors pour tout $\alpha \in C$ on a $M_v^*(\alpha) = 0$.

Le résultat principal de cette section est le suivant:

Théorème 7.6. Soit $f : Z \to B$ un morphisme dominant de k-variétés lisses et géométriquement intègres. Notons Z_η la fibre générique du morphisme, Z_η^c une compactification lisse de Z_η et $Z_{\overline{K}}^c$ son extension à $\overline{K}$ (où $\overline{K}$ est une clôture algébrique du corps des fonctions K de B). Faisons les hypothèses suivantes:

(1) le groupe $\mathrm{Br}_{\mathrm{nr}}(B)/\operatorname{Br} k$ est fini;

(2) la fibre générique Z_η admet un K-point m_k;

(3) le groupe $\mathrm{Br}(Z_{\overline{K}}^c)$ est fini;

(4) le groupe $\mathrm{Pic}(Z_{\overline{K}}^c)$ est de type fini et sans torsion;

(5) les k-fibres de f au-dessus d'un ouvert non vide de B vérifient (BMO).

Sous ces hypothèses, si B vérifie (BMO), alors Z vérifie (BMO) et $\mathrm{Br}_{\mathrm{nr}}(Z)/\operatorname{Br} k$ est fini.

Démonstration. Quitte à restreindre Z et B, on peut d'emblée supposer que f est lisse, que toutes ses fibres vérifient (BMO) et qu'il admet une section s qui étend m_K (ce dernier point suit de l'hypothèse (2) combinée à la lissité générique de f, voir [BLR90, §2.2 proposition 14]).

Commençons par remarquer que $\mathrm{Br}_{\mathrm{nr}}(Z_\eta)/\operatorname{Br}(K)$ est un groupe fini. En effet, par (2.3), on a une flèche injective

$$\ker\left\{\mathrm{Br}_{\mathrm{nr}}(Z_\eta)/\operatorname{Br}(K) \to \mathrm{Br}(Z_{\overline{K}}^c)\right\} \hookrightarrow H^1(K, \mathrm{Pic}(Z_{\overline{K}}^c))$$

De plus $H^1(K, \mathrm{Pic}(Z_{\overline{K}}^c))$ est fini car $\mathrm{Pic}(Z_{\overline{K}}^c)$ étant de type fini sur Γ_K, on peut trouver un ouvert distingué U de Γ_K qui agit trivialement sur $\mathrm{Pic}(Z_{\overline{K}}^c)$, si bien que $H^1(U, \mathrm{Pic}(Z_{\overline{K}}^c)) = 0$ (car $\mathrm{Pic}(Z_{\overline{K}}^c)$ est sans torsion) et donc $H^1(K, \mathrm{Pic}(Z_{\overline{K}}^c))$ est isomorphe à $H^1(\Gamma_k/U, \mathrm{Pic}(Z_{\overline{K}}^c))$ (voir [Ser94, I, 2.6.b)]), lequel est fini car Γ_K/U est fini et $\mathrm{Pic}(Z_{\overline{K}}^c)$ est de type fini sur Γ_K/U. Puisque $\mathrm{Br}(Z_{\overline{K}}^c)$ est également supposé fini, il vient que $\mathrm{Br}_{\mathrm{nr}}(Z_\eta)/\operatorname{Br}(K)$ est un groupe fini. On choisit alors $C \subseteq \mathrm{Br}(k(Z))$, un système de représentants de $\mathrm{Br}_{\mathrm{nr}}(Z_\eta)/\operatorname{Br}(K)$. Quitte à translater les éléments de C par des éléments de $\mathrm{Br}(K)$, on peut également supposer que $\alpha(m_k) = 0$ pour tout α dans C. Quitte à réduire B, on peut donc aussi se ramenener au cas où $\alpha(s(m)) = 0$ pour tout $m \in B$ et ce en utilisant le lemme (4.23).

Déduisons-en que $\mathrm{Br}_{\mathrm{nr}}(Z)/\operatorname{Br}(k)$ est fini. Le morphisme dominant $Z_\eta \to Z$ induit, par fonctorialité du groupe de Brauer non ramifié, un morphisme

$$\mathrm{Br}_{\mathrm{nr}}(Z)/\operatorname{Br}(k) \to \mathrm{Br}_{\mathrm{nr}}(Z_\eta)/\operatorname{Br}(K)$$

dont il s'agit de montrer que le noyau est fini. En effet, si $\alpha \in \mathrm{Br}(K)$ est tel que $f^*\alpha$ est dans $\mathrm{Br}_{\mathrm{nr}}(Z)$, alors par fonctorialité du groupe de Brauer non ramifié, il suit que $s^*f^*\alpha \in \mathrm{Br}_{\mathrm{nr}}(B)$. Mais puisque s est une section de f, on en déduit que le noyau du morphisme considéré s'injecte dans $\mathrm{Br}_{\mathrm{nr}}(B)/\operatorname{Br}(k)$, lequel est fini par hypothèse, ce qui montre la finitude de $\mathrm{Br}_{\mathrm{nr}}(Z)/\operatorname{Br}(k)$.

Il suit alors de [HW16, remark 4.4.] (admis) qu'il existe un ensemble hilbertien H de $B(k)$ tel que pour tout élément m de H, les spécialisations des éléments de C en la fibre Z_m engendrent $\mathrm{Br}_{\mathrm{nr}}(Z_m)/\mathrm{Br}(k)$.

En vertu de l'hypothèse (1) et de (4.27), B vérifie (ATF): considérons alors S_0 un ensemble fini de places en dehors duquel B vérifie l'approximation faible et contenant les places de mauvaise réduction d'un ensemble fini de représentants de $\mathrm{Br}_{\mathrm{nr}}(B)/\mathrm{Br}(k)$.

Considérons $(Q_v)_{v\in\Omega_k} \in Z(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$, qu'on veut approcher par un point de Z en un ensemble fini de places S. En vertu du «lemme formel» (6.1) on peut, quitte à réduire Z et rajouter des places à S, supposer que $\sum_{v\in S} inv_v(Q_v^*\alpha) = 0$ pour tout $\alpha \in C$. Si (P_v) désigne l'image de la famille (Q_v) par f, alors (P_v) est dans $B(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$: le choix de S_0 permet alors d'appliquer le lemme 1 sous la forme de la remarque (7.5); autrement dit, on peut trouver un point de H arbitrairement proche de $(P_v)_{v\in k_\Omega}$.

Puisque f est lisse, on peut trouver dans la fibre Z_m des points locaux Q'_v arbitrairement proches des Q_v (pour $v \in S$), si bien que $\sum_{v\in S} inv_v({Q'}_v^*\alpha) = 0$ en vertu du lemme (4.23). On complète alors la famille $(Q'_v)_{v\in S}$ en une famille $(Q'_v)_{v\in\Omega_k}$ en posant, pour $v \notin S$, $Q'_v = s(m)$. Alors, $(Q'_v)_{v\in\Omega_k}$ est proche de $(Q_v)_{v\in\Omega_k}$ en les places de S et est dans $Z_m(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$: ce dernier point suit du fait que les éléments de C engendrent le quotient $\mathrm{Br}_{\mathrm{nr}}(Z_m)/\mathrm{Br}(k)$, couplé au fait que les spécialisations des éléments de C en $s(m)$ sont nulles.

Enfin, en utilisant le fait que les k-fibres de f vérifient (BMO), on peut approcher $(Q'_v)_{v\in\Omega_k}$ par un k-point de Z aux places de S, ce qui conclut. □

Remarque 7.7. Les hypothèses (2), (3) et (4) sur f sont vérifiées si sa fibre générique est unirationnelle. L'hypothèse (1) est vérifiée si B est k-unirationnelle.

7.2 Démonstration du théorème

Rappelons l'énoncé du théorème:

Théorème 7.1. Soit

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

une extension scindée de k-groupes finis, avec A abélien. Si G vérifie (BMO), alors il en va de même pour E.

Démonstration. Faisons agir E (resp. G) fidèlement sur un espace affine $\mathbf{A}_k^n$ (resp. $\mathbf{A}_k^m$). Par le fait (0.12), choisissons X' (resp. B') un ouvert non vide de $\mathbf{A}_k^n$ (resp. $\mathbf{A}_k^m$) sur lequel E (resp. G) agit librement. On pose alors $Y = X'/A$, $X = X'/E$ et $B = B'/G$, si bien que $X = Y/G$: ici, on fait agir $g \in G$ sur Y en prenant un antécédent $e \in E$ de g et en le faisant agir sur Y, cette action étant indépendante de l'antécédent choisi. Il s'agit de montrer que X vérifie (BMO).

On considère alors Y comme un X-torseur à droite sous G et on note $Z = Y \times_k^G B'$ le produit contracté de Y et B'. Montrons que Z est stablement k-birationnelle à

$X = Y/G$. Puisque Z est un ouvert de $(Y \times_k^G \mathbf{A}_k^m)/G$, il suffit de montrer que ce dernier est stablement birationnel à X. Or, l'action libre de G sur $Y \times_k \mathbf{A}_k^m$ et sur Y (compatible à la projection) donne le diagramme cartésien

$$\begin{tikzcd} Y \times_k \mathbf{A}_k^m \arrow[r] \arrow[d] & (Y \times_k \mathbf{A}_k^m)/G \arrow[d] \\ Y \arrow[r] & X = Y/G \end{tikzcd}$$

où le morphisme $Y \to X$ est fppf en vertu de (0.22); autrement dit, le morphisme $(Y \times_k^G \mathbf{A}_k^m)/G \to X$ est un fibré vectoriel localement trivial pour la topologie fppf. Il suit de Hilbert 90 (voir [Mil80, chapter III, §4, proposition 4.9.]) que c'est un fibré vectoriel localement trivial pour la topologie de Zariski, et donc que $(Y \times_k^G \mathbf{A}_k^m)/G$ est stablement birationnellement équivalent à X. Puisqu'on veut montrer que X vérifie (BMO), il suffit donc de montrer que Z vérifie (BMO).

Considérons $f : Z \to B$ défini comme le quotient de $Y \times_k B' \to B$, lequel est donné par la composition du quotient $B' \to B$ par la projection $Y \times_k B' \to B'$. Notons $X_{k(B)} = X \otimes_k k(B)$ et $Y_{k(B)} = Y \otimes_k k(B)$. Alors la fibre générique de f est

$$Z_\eta = (Y \times_k^G B') \times_B k(B) = ((Y \times_k B) \times_B^G B') \times_B k(B) = Y_{k(B)} \times_{k(B)}^G B'_\eta$$

qui est le tordu $(Y_{k(B)})^S$ de $Y_{k(B)}$ par le G-torseur à gauche $B'_\eta \xrightarrow{S} \eta$.

Fixons $\sigma : G \to E$ une section de la suite exacte de l'énoncé et considérons le $E_{k(B)}$-torseur à gauche $T = E_{k(B)} \times_{k(B)}^G B'_\eta$, où $E_{k(B)}$ est un $(E_{k(B)}, G_{k(B)})$ bitorseur défini par $e.x.g = ex\sigma(g)$. Alors, remarquons que le tordu de $X'_{k(B)} \to Y_{k(B)}$, sur lequel $E_{k(B)}$ agit à droite, par T est

$$(X'_{k(B)})^T = X'_{k(B)} \times_{k(B)}^{E_{k(B)}} (E_{k(B)} \times_{k(B)}^{G_{k(B)}} B'_\eta) = X'_{k(B)} \times_{k(B)}^{G_{k(B)}} B'_\eta \to Y_{k(B)} \times_{k(B)}^{G_{k(B)}} B'_\eta = Z_\eta$$

et on peut faire agir le groupe tordu $(A_{k(B)})^T = A_{k(B)} \times_{k(B)}^{G_{k(B)}} B'_\eta$ sur $(X'_{k(B)})^T = X'_{k(B)} \times_{k(B)}^{G_{k(B)}} B'_\eta$ par $(x, b).(a, b) := (xa, b)$, cette action étant bien définie car

$$(x\sigma(g), g^{-1}b).(\sigma(g)^{-1}a\sigma(g), g^{-1}b) = (xa\sigma(g), g^{-1}b) = (xa, b).$$

De la sorte, $(X'_{k(B)})^T \to Z_\eta$ est un $(A_{k(B)})^T$-torseur. Il suit donc que Z_η est un ouvert du quotient de $(\mathbf{A}_{k(B)}^n)^T$ par $(A_{k(B)})^T$. Mais puisque $(\mathbf{A}_{k(B)}^n)^T$ est $k(B)$-isomorphe à $\mathbf{A}_{k(B)}^n$ (par Hilbert 90), on en en déduit que Z_η est birationnelle à $\mathbf{A}_{k(B)}^n/(A_{k(B)})^T$ et donc que Z_η est $k(B)$-unirationnelle.

De même, si b est un k-point de B, la fibre Z_b de f en b est isomorphe à un ouvert du quotient de $(\mathbf{A}_k^n)^{T'}$ par le groupe abélien $A^{T'}$, où $T' = E \times_k^G B'_b$: en vertu du théorème (4.28), les k-fibres de f vérifient donc également (BMO).

De plus, B est unirationnelle donc $\mathrm{Br}_{\mathrm{nr}}(B)/\mathrm{Br}(k)$ est fini. Ainsi, les hypothèses du théorème (7.6) sont vérifiées, au regard de la remarque (7.7): il suit donc que Z

vérifie (BMO). Il en va donc de même pour X, d'où on conclut que l'obstruction de Brauer-Manin est la seule à l'approximation faible pour E. $\square$

Références

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[Bor96] Mikhail Borovoi. The Brauer-Manin obstructions for homogeneous spaces with connected or abelian stabilizer. *J. Reine Angew. Math.*, 473:181–194, 1996.

[Con12] Brian Conrad. Weil and Grothendieck approaches to adelic points. *Enseign. Math. (2)*, 58(1-2):61–97, 2012.

[CTO89] Jean-Louis Colliot-Thélène and Manuel Ojanguren. Variétés unirationnelles non rationnelles: au-delà de l'exemple d'Artin et Mumford. *Invent. Math.*, 97(1):141–158, 1989.

[CTS07] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group). In *Algebraic groups and homogeneous spaces*, volume 19 of *Tata Inst. Fund. Res. Stud. Math.*, pages 113–186. Tata Inst. Fund. Res., Mumbai, 2007.

[Del77] P. Deligne. *Cohomologie étale*, volume 569 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1977. Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$.

[Del80] Pierre Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980.

[Eke90] Torsten Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 241–249. Birkhäuser Boston, Boston, MA, 1990.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[FK88] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné.

[Gab94] Ofer Gabber. Affine analog of the proper base change theorem. *Israel J. Math.*, 87(1-3):325–335, 1994.

[GGK$^+$68] J. Giraud, A. Grothendieck, S. L. Kleiman, M. Raynaud, and J. Tate. *Dix exposés sur la cohomologie des schémas*, volume 3 of *Advanced Studies in*

Pure Mathematics. North-Holland Publishing Co., Amsterdam; Masson & Cie, Editeur, Paris, 1968.

[GP11] Philippe Gille and Patrick Polo, editors. *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*, volume 7 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, 2011. Séminaire de Géométrie Algébrique du Bois Marie 1962–64. [Algebraic Geometry Seminar of Bois Marie 1962–64], A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre, Revised and annotated edition of the 1970 French original.

[Gro67] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[Har94] David Harari. Méthode des fibrations et obstruction de Manin. *Duke Math. J.*, 75(1):221–260, 1994.

[Har07] David Harari. Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini. *Bull. Soc. Math. France*, 135(4):549–564, 2007.

[Hir64] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II. *Ann. of Math. (2)* **79** *(1964), 109–203; ibid. (2)*, 79:205–326, 1964.

[HW16] Yonatan Harpaz and Olivier Wittenberg. On the fibration method for zero-cycles and rational points. *Ann. of Math. (2)*, 183(1):229–295, 2016.

[HW18] Yonatan Harpaz and Olivier Wittenberg. Zéro-cycles sur les espaces homogènes et problème de Galois inverse. *arXiv e-prints*, page arXiv:1802.09605, Feb 2018.

[Kra84] Hanspeter Kraft. *Geometrische Methoden in der Invariantentheorie*. Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig, 1984.

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[Mil17] J. S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.

[Neu73] Jürgen Neukirch. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.*, 21:59–116, 1973.

[Neu79] Jürgen Neukirch. On solvable number fields. *Invent. Math.*, 53(2):135–164, 1979.

[Noe17] Emmy Noether. Gleichungen mit vorgeschriebener Gruppe. *Math. Ann.*, 78(1):221–229, 1917.

[Pin97] Richard Pink. The Mumford-Tate conjecture for Drinfeld-modules. *Publ. Res. Inst. Math. Sci.*, 33(3):393–425, 1997.

[Poo17] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[Sal82] David J. Saltman. Generic Galois extensions and problems in field theory. *Adv. in Math.*, 43(3):250–283, 1982.

[Ser94] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Ser06] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006. 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition.

[Ser08] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.

[Sko01] Alexei Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.

[Swa83] Richard G. Swan. Noether's problem in Galois theory. In *Emmy Noether in Bryn Mawr (Bryn Mawr, Pa., 1982)*, pages 21–40. Springer, New York-Berlin, 1983.

[Voi19] Claire Voisin. *Birational invariants and decomposition of the diagonal*. 2019.

[Vos73] V. E. Voskresenskiĭ. Fields of invariants of abelian groups. *Uspehi Mat. Nauk*, 28(4(172)):77–102, 1973.