Groupe de Brauer non-ramifié d'espaces homogènes à stabilisateurs finis

Cyril Demarche

Résumé

On s'intéresse dans ce texte au groupe de Brauer d'une compactification lisse d'un espace homogène d'un groupe semi-simple simplement connexe à stabilisateurs finis, sur un corps de nombres, ainsi qu'aux liens existants entre l'obstruction de Brauer-Manin à l'approximation faible sur un tel espace homogène et la cohomologie galoisienne du stabilisateur. On montre notamment une formule décrivant ce groupe de Brauer, dit non-ramifié, et on construit des familles d'exemples et de contrexemples pour lesquels ce groupe de Brauer non-ramifié coïncide ou non avec le sous-groupe du groupe de Brauer formé des éléments localement constants en presque tout place. Enfin, on démontre que le fait que l'obstruction de Brauer-Manin à l'approximation faible soit la seule est équivalent à une condition simple sur la cohomologie galoisienne du stabilisateur.

1 Introduction

On s'intéresse ici aux espaces homogènes d'un groupe algébrique semi-simple simplement connexe sur un corps de nombres, dont le stabilisateur (géométrique) est fini. On s'intéresse notamment au groupe de Brauer non-ramifié de ces espaces. Plus précisément, étant donné un corps de nombres k, et G un k-groupe algébrique fini, on se donne un plongement de G dans $\mathbf{SL}_{n,k}$ (dans toute cette construction, on peut remplacer $\mathbf{SL}_n$ par $\mathbf{GL}_n$, les variétés obtenues étant alors k-stablement birationnelles), et on définit l'espace homogène quotient $X := \mathbf{SL}_n/G$. Cette variété ne dépend pas, à k-stable-birationalité près, de la représentation fidèle de G choisie (c'est le lemme sans nom, voir par exemple [6], corollaire 3.9). De plus, X est une k-variété lisse géométriquement intègre. On s'intéresse à l'arithmétique de la variété X. On sait qu'en général, la variété X ne vérifie pas l'appoximation faible, c'est à dire que l'adhérence de $X(k)$ dans $X(k_\Omega) := \prod_{v\in\Omega_k} X(k_v)$ (muni de la topologie produit direct des topologies v-adiques, v décrivant l'ensemble Ω_k des places de k) n'est pas toujours l'ensemble $X(k_\Omega)$ tout entier. Pour étudier le défaut d'approximation faible, on utilise l'obstruction de Brauer-Manin : si $\mathrm{Br}_{\mathrm{nr}}(X)$ est le groupe de Brauer cohomologique [1] d'une compactification lisse de X, on dispose d'un accouplement naturel (voir par exemple [26], section 5.2)

$$\begin{array}{ccc} X(k_\Omega) \times \mathrm{Br}_{\mathrm{nr}}(X) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ ((P_v), A) & \longmapsto & \langle A, (P_v) \rangle_{\mathrm{BM}} := \sum_{v \in \Omega_k} j_v(A(P_v)) \end{array}$$

tel que l'adhérence de $X(k)$ dans $X(k_\Omega)$ soit contenue dans le noyau à gauche $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)}$ de cet accouplement (pour ce résultat, voir par exemple [26], pages 102-103).

Étant donné un sous-groupe B de $\mathrm{Br}_{\mathrm{nr}}(X)$, on se demande alors si l'obstruction de Brauer-Manin relative à B à l'approximation faible est la seule pour X, c'est-à-dire si l'adhérence de $X(k)$ dans $X(k_\Omega)$ coïncide avec l'ensemble

$$X(k_\Omega)^B := \{(P_v) \in X(k_\Omega) : \langle A, (P_v) \rangle_{\mathrm{BM}} = 0 \text{ pour tout } A \in B\}$$

Dans le cas où le groupe G est connexe ou abélien, ce résultat est connu et dû à Borovoi en prenant pour B le sous-groupe $Б_\omega(X)$ formés des éléments localement constants (voir [4], corollaire 2.5 par exemple). En revanche, quand le groupe G est fini, peu de résultats sont connus : on sait que si le groupe G est abélien fini, alors l'obstruction de Brauer-Manin sur X est la seule (voir par exemple [23], lemme 1.4), et on sait que la variété X vérifie l'approximation faible si G est constant résoluble d'ordre impair sur $\mathbf{Q}$ (c'est un résultat dû à Neukirch, voir [18], corollaire 9.3, et [19], corollaire 2). Mais le problème général reste ouvert : en fait, hormis les résultats cités et les cas traités dans [10], il semble qu'on ne dispose d'aucun résultat sur le sujet, notamment par exemple pour les groupes constants non-abéliens d'ordre pair (en particulier dans le cas des groupes finis parfaits). L'une des motivations pour étudier ce problème pour des groupes G finis est le problème de Galois-inverse, comme expliqué dans la section 4 de [10]. Dans ce texte, on s'intéresse au groupe de Brauer non-ramifié de ces variétés, dans d'autres cas que ceux considérés jusqu'ici.

Dans tout ce texte, $\overline{k}$ désigne une clôture algébrique de k, Γ_k est le groupe de Galois absolu du corps k, à savoir $\Gamma_k := \mathrm{Gal}(\overline{k}|k)$. Si X est une k-variété et si K/k est une extension de corps, on note $X_K := X \times_k K$ la K-variété obtenue à partir de X par extension des scalaires de k à K. On définit également $\overline{X} := X \times_k \overline{k}$, et $\mathrm{Br}_1(X) := \mathrm{Ker}(\mathrm{Br}\, X \to \mathrm{Br}\, \overline{X})$. On notera également $\mathrm{Br}_{\mathrm{nr}}(X)$ le groupe de Brauer non-ramifié de X, c'est-à-dire le groupe de Brauer d'une compactification lisse de X, et $\mathrm{Br}_{\mathrm{nr}_1}(X)$ le noyau de $\mathrm{Br}_{\mathrm{nr}}(X) \to \mathrm{Br}_{\mathrm{nr}}(\overline{X})$.

Si $X := \mathbf{SL}_n/G$ est le quotient de $\mathbf{SL}_{n,k}$ par un k-sous-groupe fini G, on définit Z comme le quotient de $\mathbf{SL}_n$ par le sous-groupe dérivé $D(G)$ de G. Z est un X-torseur

[1] Dans tout le texte, le groupe de Brauer d'une k-variété Y est par définition le groupe $\mathrm{Br}(Y) := H^2_{\text{ét}}(Y, \mathbf{G}_m)$

sous G^{ab}, et on a le diagramme suivant :

$$\begin{tikzcd} \mathbf{SL}_n \arrow[dd, "G"'] \arrow[dr, "D(G)"] & \\ & Z \arrow[dl, "G^{\mathrm{ab}}"] \\ X & \end{tikzcd}$$

On note M est le Γ_k-module dual de G^{ab}, défini par $M := \mathrm{Hom}_{\overline{k}}(G^{\mathrm{ab}}, \overline{k}^*)$, avec l'action de Γ_k suivante : $({}^{\gamma}\varphi)(h) := {}^{\gamma}(\varphi({}^{\gamma^{-1}}h))$ pour tout $\gamma \in \Gamma_k$, $\varphi \in M$ et $h \in G^{\mathrm{ab}}(\overline{k})$. On sait (voir par exemple [26], théorème 4.1.1) que le groupe $\mathrm{Br}_1(X)/\mathrm{Br}(k)$ s'identifie à $H^1(k, M)$ et que tout élément de $\mathrm{Br}_1(X)$ s'obtient comme un cup-produit $a \cup [Z] + \alpha_0$, pour $a \in H^1(k, M)$ et $\alpha_0 \in \mathrm{Br}\ k$, où $[Z]$ désigne la classe de Z dans $H^1(X, G^{\mathrm{ab}})$. On note $\text{Б}_\omega(X)$ le sous-groupe de $\mathrm{Br}_1(X)$ correspondant au sous-groupe $\text{Ш}^1_\omega(k, M)$ de $H^1(k, M)$ formé des éléments de $H^1(k, M)$ dont la restriction est nulle dans $H^1(k_v, M)$ pour presque toute place v de k (dans tout le texte, l'expression "pour presque toute place de k" signifie "pour toutes les places de k, sauf un nombre fini d'entre elles"). C'est un sous-groupe de $\mathrm{Br}_{\mathrm{nr}_1}(X)$ (cf [9], théorème 2.1.1), qui correspond aux éléments $\alpha \in \mathrm{Br}_1(X)$ tels que $\alpha_v \in \mathrm{Br}_1(X_{k_v})$ provienne de $\mathrm{Br}(k_v)$ pour presque toute place v de k.

On cherche ici à calculer explicitement les groupes $\text{Б}_\omega(X)$ et $\mathrm{Br}_{\mathrm{nr}_1}(X)$ dans des cas particuliers, ainsi que les obstructions à l'approximation faible correspondantes, à savoir les ensembles $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)}$ et $X(k_\Omega)^{\text{Б}_\omega(X)}$, le premier étant naturellement contenu dans le second.

Ainsi les questions que l'on se pose sont les suivantes : l'obstruction de Brauer-Manin algébrique à l'approximation faible est-elle la seule sur X, i.e. l'adhérence de $X(k)$ dans $X(k_\Omega)$ est-elle exactement $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)}$? Les ensembles $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)}$ et $X(k_\Omega)^{\text{Б}_\omega(X)}$ coïncident-ils ? Les groupes $\mathrm{Br}_{\mathrm{nr}_1}(X)$ et $\text{Б}_\omega(X)$ sont-ils égaux ? Comme mentionné plus haut, très peu de résultats sont connus à propos de ce problème, notamment dans les cas où le groupe G est fini, non-abélien et d'ordre pair. Dans ce texte, on cherche à décrire le groupe $\mathrm{Br}_{\mathrm{nr}_1}(X)$, à le comparer au groupe $\text{Б}_\omega(X)$, et à interpréter l'obstruction associée à $\mathrm{Br}_{\mathrm{nr}_1}(X)$ en terme de la cohomologie galoisienne du groupe G.

Dans la première partie, on va montrer une formule reliant le groupe de Brauer non-ramifié de X à la cohomologie galoisienne de G, formule généralisant la proposition 4 de [10]. Dans la deuxième partie, on exploite cette formule dans le cas des groupes G finis constants, et on montre dans la partie 3 un résultat de trivialité pour $\mathrm{Br}_{\mathrm{nr}_1}(X)$ dans le cas où G est un p-groupe constant d'un certain type. Dans la section 4, on compare les groupes $\mathrm{Br}_{\mathrm{nr}_1}(X)$ et $\text{Б}_\omega(X)$, sous certaines hypothèses concernant le cardinal du groupe fini G et les racines de l'unité dans k. Dans la cinquième partie, on répond à une question de Harari (voir [10], question avant la proposition 4) en construisant un p-groupe (fini) constant G pour lequel $\text{Б}_\omega(X)$ est trivial, mais $\mathrm{Br}_{\mathrm{nr}_1}(X)$ ne l'est pas, et pour lequel $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)} \subsetneq X(k_\Omega)^{\text{Б}_\omega(X)} = X(k_\Omega)$: en cela le cas des espaces homogènes à stabilisateurs finis diffère nettement du cas des espaces homogènes à stabilisateurs connexes ou abéliens, cas dans lequel les deux groupes $\text{Б}_\omega(X)$ et $\mathrm{Br}_{\mathrm{nr}_1}(X)$ coïncident (voir par exemple [5], théorème A). L'exemple de cette partie est donc d'une nature assez nouvelle : c'est un espace homogène ne vérifiant pas l'approximation faible, et pour lequel l'obstruction de Brauer-Manin associée au groupe $\text{Б}_\omega(X)$ est insuffisante pour expliquer ce défaut d'approximation faible ; toutefois, pour cet exemple, l'obstruction à l'approximation faible associée au groupe $\mathrm{Br}_{\mathrm{nr}_1}(X)$ est bien la seule. Dans la partie 6, on donne au théorème 7.1 une formule permettant de calculer explicitement l'obstruction de Brauer-Manin sur X relative à $\mathrm{Br}_{\mathrm{nr}_1}(X)$, en termes de la cohomologie galoisienne de G et de son abélianisé G^{ab}. Enfin, dans la dernière partie, on traite l'exemple particulier du groupe $G = Q_{16}$, groupe des quaternions d'ordre 16, vu comme groupe constant sur $\mathbf{Q}$.

Remarque 1.1. Dans tout ce texte, les groupes finis seront toujours considérés comme des groupes algébriques constants.

2 Formule générale pour le groupe de Brauer non-ramifié

Dans l'introduction, on a considéré des espaces homogènes de $\mathbf{SL}_n$ qui sont quotients de $\mathbf{SL}_{n,k}$, c'est-à-dire des espaces homogènes admettant un point rationnel. On va donner ici (voir le théorème 2.1) une formule générale pour le groupe de Brauer non-ramifié d'un espace homogène quelconque à stabilisateur fini, que celui-ci admette ou non un point rationnel.

Avant d'énoncer le résultat, on rappelle que, si v est une place de k, M est un Γ_{k_v}-module fini, et M' est son module dual, on dispose de l'accouplement local obtenu grâce au cup-produit :

$$H^1(k_v, M) \times H^1(k_v, M') \to \mathrm{Br}\ k_v \xrightarrow{j_v} \mathbf{Q}/\mathbf{Z}$$

où j_v est l'invariant donné par la théorie du corps de classes local (j_v est un morphisme injectif pour toute place v de k, et c'est un isomorphisme si v est une place finie). Cet accouplement est un accouplement non-dégénéré de groupes finis (voir par exemple [21], théorème 7.2.9). En outre, si le module M est non-ramifié en la place v, les sous-groupes $H^1_{\mathrm{nr}}(k_v, M)$ et $H^1_{\mathrm{nr}}(k_v, M')$ sont les orthogonaux respectifs l'un de l'autre pour cet accouplement (voir par exemple [25] section 5.5, pour la définition des groupes de cohomologie non-ramifiée).

Théorème 2.1. *Soit k un corps de nombres, G'/k un groupe algébrique semi-simple simplement connexe. Soit X un espace homogène de G', $\overline{G}$ le stabilisateur d'un point géométrique de X, que l'on supposera fini. On note également G^{ab} la k-forme du quotient de $\overline{G}$ par son sous-groupe dérivé canoniquement associée à X, et M le Γ_k-module dual de G^{ab}. Alors :*

- *Pour presque toute place v de k, X_{k_v} est k_v-isomorphe à un quotient de G'_{k_v} par un sous-groupe fini G_v de G'_{k_v}*
- *Il existe un isomorphisme naturel $r : \mathrm{Br}_1(X)/\mathrm{Br}(k) \to H^1(k, M)$ tel qu'un élément $\alpha \in \mathrm{Br}_1(X)$ est non-ramifié si et seulement si pour presque toute place v, $r(\alpha)_v \in H^1(k_v, M)$ est orthogonal à $\mathrm{Im}(H^1(k_v, G_v) \to H^1(k_v, G^{\mathrm{ab}}))$ (pour l'accouplement donné par le cup-produit).*

Ce résultat généralise la proposition 4 de [10], qui fournit la formule suivante dans le cas où $X(k) \neq \emptyset$:

Théorème 2.2 (Harari)**.** *Avec les notations du théorème 2.1, et sous l'hypothèse supplémentaire que $X(k) \neq \emptyset$, le groupe $\mathrm{Br}_{\mathrm{nr}_1}(X)/\mathrm{Br}(k)$ s'identifie au sous-groupe de $H^1(k, M)$ formé des éléments a tels que : pour presque toute place v de k, la restriction $a_v \in H^1(k_v, M)$ est orthogonale (pour le cup-produit) au sous-ensemble $\mathrm{Im}(H^1(k_v, G) \to H^1(k_v, G^{\mathrm{ab}}))$ de $H^1(k_v, G^{\mathrm{ab}})$.*

Démonstration : Suivant Springer, on considérera le k-lien L_X sur $\overline{G}$ associé à X, et la classe de Springer de X : $\alpha_X \in H^2(k, L_X)$ (voir par exemple [3], (5.1) ou [7], 7.7 pour les définitions de L_X et α_X). En remarquant que le sous-groupe dérivé de $\overline{G}$, noté $D(\overline{G})$, est invariant par les automorphismes semi-linéaires de $\overline{G}$, on en déduit que le lien L_X induit un k-lien L'_X sur le quotient $\overline{G}^{\mathrm{ab}} := \overline{G}/D(\overline{G})$, qui est un groupe abélien, et donc ce lien définit une k-forme G^{ab} de $\overline{G}^{\mathrm{ab}}$. M désigne alors le Γ_k-module dual du groupe G^{ab}.

Considérant la situation géométrique, on a un diagramme sur $\overline{k}$:

$$\begin{tikzcd}
\overline{G'} \arrow[dr] \arrow[dd, "\overline{G}"'] & \\
& \overline{Z} \arrow[dl, "\overline{G}^{\mathrm{ab}}"] \\
\overline{X} &
\end{tikzcd}$$

G' et X étant géométriquement intègres, on dispose de la suite exacte suivante (voir par exemple [26], section 2.2, suite exacte (2.8)) :

$$1 \to \overline{k}[X]^*/\overline{k}^* \to \overline{k}[G']^*/\overline{k}^* \to M \to \mathrm{Pic}(\overline{X}) \to \mathrm{Pic}(\overline{G'})$$

Or G' est semi-simple connexe, donc le lemme de Rosenlicht (cf [23], lemme 6.5) assure que $\overline{k}[G']^*/\overline{k}^* = 0$, et G' étant aussi simplement connexe, on sait que $\mathrm{Pic}(\overline{G'}) = 0$ (voir [23], lemme 6.9). On en déduit donc que $\overline{k}[X]^* = \overline{k}^*$ et $\mathrm{Pic}(\overline{X}) \cong M$. Notons $\lambda : M \to \mathrm{Pic}(\overline{X})$ cet isomorphisme (de groupes abéliens a priori).

On vérifie alors qu'en fait λ est le type du torseur $\overline{Z} \xrightarrow{\overline{G}^{\mathrm{ab}}} \overline{X}$, et que λ est un isomorphisme de Γ_k-modules (c'est un résultat dû à Borovoi, voir par exemple [26], section 9.5, preuve du théorème 9.5.1).

Enfin, le fait que les seules fonctions inversibles sur $\overline{X}$ soient les constantes assure que l'on a un isomorphisme

$$r : \mathrm{Br}_1(X)/\mathrm{Br}\ k \xrightarrow{\simeq} H^1(k, \mathrm{Pic}(\overline{X}))$$

(on peut obtenir cet isomorphisme par exemple à partir de la suite spectrale de Hochschild-Serre : voir par exemple [23], lemme 6.3.(iii) ou [26], corollaire 2.3.9). On a donc finalement montré que

$$\mathrm{Br}_1(X)/\mathrm{Br}\ k \cong H^1(k, M)$$

Dans toute cette discussion, on ne suppose pas que l'espace X possède un point rationnel sur k. Mais on sait tout de même, grâce aux estimées de Lang-Weil (X est géométriquement intègre) et au lemme de Hensel, que pour presque tout place v de k, $X(k_v) \neq \emptyset$. Notons S un ensemble fini de places de k contenant les places archimédiennes, tel que pour toute place v hors de S, $X(k_v) \neq \emptyset$. En une place $v \notin S$, on sait que X_{k_v} est isomorphe à un quotient G'_{k_v}/G_v, où G_v est une k_v-forme de $\overline{G} \times_{\overline{k}} \overline{k_v}$. Aussi, en une telle place, on a un dessin de la forme :

$$\begin{tikzcd} G'_{k_v} \arrow[dd, "G_v"'] \arrow[dr] & \\ & Z_v \arrow[dl, "G_v^{\mathrm{ab}}"] \\ X_{k_v} & \end{tikzcd}$$

On remarque que nécessairement G_v^{ab} n'est autre que $G^{\mathrm{ab}} \times_k k_v$.

On utilise alors un résultat de Harari (voir [9], théorème 2.1.1) qui caractérise les éléments non-ramifiés dans le groupe de Brauer de X : un élément $\alpha \in \mathrm{Br}_1(X)$ est non-ramifié si et seulement si pour presque toute place v de k, l'application d'évaluation

$$\begin{array}{ccc} X(k_v) & \longrightarrow & \mathrm{Br}\ k_v \\ P_v & \longmapsto & \alpha(P_v) \end{array}$$

est l'application nulle.

Or, le torseur $Z_v \to X_{k_v}$ étant universel (voir [11], preuve de la proposition 5.5), tout élément $\alpha_v \in \mathrm{Br}\, X_{k_v}$ s'écrit sous la forme $\alpha_v = p^*(a_v) \cup [Z_v] + \alpha_0$, où $p : X_{k_v} \to \mathrm{Spec}\, k_v$ est le morphisme structural, $a_v \in H^1(k_v, M)$, $[Z_v]$ est la classe du X_{k_v}-torseur Z_v dans $H^1(X_{k_v}, G_v^{\mathrm{ab}})$ et $\alpha_0 \in \mathrm{Br}\, k_v$ (pour ce résultat, voir par exemple [26], théorème 4.1.1). De plus, l'élément a_v correspond à l'élément $r(\alpha)_v$ dans $H^1(k_v, M)$, via l'isomorphisme $r : \mathrm{Br}_1(X)/\mathrm{Br}\, k \xrightarrow{\simeq} H^1(k, M)$.

On en déduit donc la caractérisation suivante : $\alpha \in \mathrm{Br}_1(X)$ est non-ramifié si et seulement si pour presque toute place v hors de S, $a_v \cup [Z_v](P_v) = 0$ pour tout point $P_v \in X(k_v)$ (où $[Z_v](P_v)$ désigne la classe dans $H^1(k_v, G^{\mathrm{ab}})$ de la fibre de $Z_v \to X_v$ en P_v) ; or $H^1(k_v, G') = 0$ (voir [14] et [15]), donc le torseur $G_{k_v} \xrightarrow{H_v} X_{k_v}$ est versel (pour la définition de cette notion, voir par exemple [8], sections 5.1 et 5.3), donc quand P_v décrit l'ensemble $X(k_v)$, $[Z_v](P_v)$ décrit exactement $\mathrm{Im}(H^1(k_v, G_v) \to H^1(k_v, G^{\mathrm{ab}}))$. D'où finalement la caractérisation du théorème 2.1. □ □

Remarque 2.3. La description générale donnée au théorème 2.1 n'est pas complétement explicite quand L_X ne provient pas d'une k-forme de $\overline{G}$, puisque dans ce cas les k_v-formes G_v sont définies seulement localement, et ne proviennent pas d'une même k-forme a priori, ce qui rend sans doute plus difficile le calcul de $\mathrm{Br}_{\mathrm{nr}\ 1}(X)$ que dans le cas du théorème 2.2.

Dans la suite de ce texte, on sera dans le cadre du théorème 2.2.

3 Sur la flèche $H^1(F,G) \to H^1(F,G^{\mathrm{ab}})$, F corps p-adique

Dans cette partie, on considère un groupe fini G, vu comme groupe algébrique constant, et la variété $X = \mathbf{SL}_n/G$ associée. À la vue du théorème 2.2, il semble légitime de s'intéresser à l'application $H^1(k_v, G) \to H^1(k_v, G^{\mathrm{ab}})$, et notamment aux cas dans lesquels cette application est surjective. Dans le cas où G est un groupe constant, cette flèche est assez explicite.

Si F est un corps quelconque, et G un groupe constant, l'application d'ensembles pointés $H^1(F,G) \to H^1(F,G^{\mathrm{ab}})$, s'identifie à l'application

$$\mathrm{Hom}_{\mathrm{cont.}}(\Gamma_F, G)/\sim\; \to \mathrm{Hom}_{\mathrm{cont.}}(\Gamma_F, G^{\mathrm{ab}})$$

la relation d'équivalence considérée étant la conjugaison par un élément de G.

Désormais, dans cette section, F est un corps p-adique. Dans ce cas, étant donné un morphisme de groupes continu $\phi : \Gamma_F \to G$, si l'on suppose que p ne divise pas le cardinal de G, alors ce morphisme se factorise au travers du plus grand quotient modérement ramifié Γ_0 de Γ_F, et par conséquent on est ramené à étudier la flèche

$$\mathrm{Hom}_{\mathrm{cont.}}(\Gamma_0, G)/\sim \longrightarrow \mathrm{Hom}_{\mathrm{cont.}}(\Gamma_0, G^{\mathrm{ab}})$$

où Γ_0 est le groupe de Galois de l'extension maximale modérement ramifiée F^{tr} de F, i.e. $\Gamma_0 = \mathrm{Gal}(F^{\mathrm{tr}}|F)$. Or on connaît la structure du groupe profini Γ_0 (voir par exemple [21], théorèmes 7.5.1 et 7.5.2) : Γ_0 est le groupe profini engendré par deux générateurs σ et τ soumis à la seule relation $\sigma\tau\sigma^{-1} = \tau^q$, où q est le cardinal du corps résiduel de F. Considérant toujours $\phi : \Gamma_0 \to G'$ (G' est un groupe fini quelconque), ϕ est alors entièrement déterminé par les images respectives $\overline{a}$ et $\overline{b}$ des générateurs σ et τ, et ainsi se donner un tel morphisme revient à se donner deux éléments $\overline{a}$ et $\overline{b}$ de G' vérifiant la relation $\overline{a}\overline{b}\overline{a}^{-1} = \overline{b}^q$ (on remarque également qu'un élément de $H^1(F,G')$ est non-ramifié si et seulement si tout morphisme $\phi : \Gamma_0 \to G'$ le représentant vérifie $\phi(\tau) = 1$). Finalement, un morphisme $\phi : \Gamma_F \to G^{\mathrm{ab}}$, donné par des éléments $\overline{a}$ et $\overline{b}$ de G^{ab} vérifiant $\overline{b}^{q-1} = 1$, se relève en un morphisme $\Gamma_F \to G$ si et seulement si les éléments $\overline{a}$ et $\overline{b}$ se relèvent respectivement en des éléments a et b de G tels que $aba^{-1} = b^q$.

En particulier, on peut se poser la question suivante : soit G un groupe fini, soit G^{ab} son abélianisé. Soit l un nombre premier et $\overline{g} \in G^{\mathrm{ab}}$ tel que $\overline{g}^{l-1} = 1$. Peut-on relever $\overline{g}$ en un élément $g \in G$ de sorte que g^l soit conjugué à g ?

Montrons d'abord qu'en toute généralité, la réponse ne peut être positive.

Proposition 3.1. *Pour tout nombre premier p, et pour tout entier $n > p$, il existe un p-groupe fini G de cardinal p^n (et de classe de nilpotence maximale, à savoir que la série centrale descendante de G est de longueur maximale, donc égale à $n-1$), tel qu'il existe $\overline{g} \in G^{\mathrm{ab}}$ et une infinité de nombres premiers l pour lesquels $\overline{g}^{l-1} = 1$, mais $\overline{g}$ ne se relève pas en un élément g de G tel que g^l soit conjugué à g.*

Démonstration :

- Cas $p = 2$.
  On note $k := 2^{n-1}$ et on considère le groupe diédral $G := \mathbf{D}_k$, d'ordre $2k = 2^n$. C'est le produit semi-direct de $\mathbf{Z}/k\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$, l'élément non-trivial de $\mathbf{Z}/2\mathbf{Z}$ agissant sur $\mathbf{Z}/k\mathbf{Z}$ par multiplication par -1. On a une présentation de ce groupe donnée par les deux générateurs r et s soumis aux relations suivantes $r^k = 1$, $s^2 = 1$ et $srs = r^{-1}$. Le sous-groupe dérivé de G est clairement le sous-groupe de G engendré par r^2. Par conséquent, l'abélianisé de G s'identifie au produit direct $\langle r\rangle/\langle r^2\rangle \times \langle s\rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On considère alors l'élément $\overline{g} := (1,0) \in G^{\mathrm{ab}}$. Alors pour tout l premier impair on a $\overline{g}^{l-1} = 1$ dans G^{ab}. Soit $g := (r^{2t+1}, 0)$, $t \in \mathbf{Z}/k\mathbf{Z}$ un relevé de $\overline{g}$ dans G et supposons que sa puissance l-ième soit conjuguée à g. Un calcul rapide assure que les seuls conjugués de g sont g et g^{-1}. Par conséquent, g^l conjugué à g signifie que k divise $(l-1)(2t+1)$ ou k divise $(l+1)(2t+1)$. Or $k = 2^{n-1}$, donc cela équivaut au fait que 2^{n-1}

divise $(l-1)$ ou $(l+1)$. Or le théorème de la progression arithmétique assure qu'il existe une infinité de nombres premiers l tels que 4 divise $l-1$ et 2^{n-1} ne divise pas $l-1$ (les nombres premiers l vérifiant ces conditions ont une densité $\frac{1}{2} - \frac{1}{2^{n-2}} > 0$). Or pour un tel nombre l, 2^{n-1} ne divise pas non plus $l+1$ puisque $l+1$ est de valuation 2-adique égale à 1. Par conséquent, tous ces nombres premiers l (qui sont en nombre infini) fournissent des contrexemples à la propriété de relèvement étudiée.

– Cas $p \geq 3$.
On considère une généralisation naturelle du groupe diédral : on notera E_{p^n} le groupe de cardinal p^n défini par $E_{p^n} := \mathcal{O}_p/\mathfrak{p}_p^{n-1} \rtimes C_p$, avec les notations suivantes :
  - $K_p := \mathbf{Q}_p(\zeta)$, où ζ est une racine primitive p-ième de l'unité.
  - $\mathcal{O}_p$ est l'anneau des entiers de K_p.
  - $\mathfrak{p}_p$ est l'idéal maximal de $\mathcal{O}_p$, engendré par $\theta := 1-\zeta$.
  - C_p est le groupe des racines p-ièmes de l'unité dans K_p, i.e. le groupe cyclique d'ordre p engendré par ζ.
  - l'élément ζ de C_p agit sur $\mathcal{O}_p$ par multiplication par ζ. Pour cette action, l'idéal $\mathfrak{p}_p$ est stable.
  - v_p désigne la valuation p-adique usuelle, étendue à K_p. Puisque l'extension est totalement ramifiée, on a $v_p(p) = 1$ et $v_p(\theta) = \frac{1}{p-1}$.

Calculons le sous-groupe dérivé de $G := E_{p^n}$. Si on note x et y des éléments de $\mathcal{O}_p$, et $\overline{x}$ et $\overline{y}$ leurs classes respectives modulo $\mathfrak{p}_p^{n-1}$, on a :

$$[(\overline{x},\zeta^r),(\overline{y},\zeta^s)] = (\theta(\overline{x}(1+\zeta+\cdots+\zeta^{s-1}) - \overline{y}(1+\zeta+\cdots+\zeta^{r-1})),1)$$

Donc le groupe dérivé est $D(G) = \mathfrak{p}_p\mathcal{O}_p/\mathfrak{p}_p^{n-1}$. Par conséquent l'abélianisé de G est

$$G^{\mathrm{ab}} \cong \mathcal{O}_p/\mathfrak{p}_p \times C_p \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$$

Considérons alors l'élément $\overline{g} := (1,0)$ de $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ correspondant à l'élément $(1,1) \in \mathcal{O}_p/\mathfrak{p}_p \times C_p$, le premier 1 désignant la classe de 1. Un relevé de $\overline{g}$ est de la forme $g = (1+\theta x \bmod {\mathfrak{p}_p}^{n-1}, 1)$. La puissance l-ième de g est conjuguée à g si et seulement si $l(1+\theta x) \equiv \zeta^r(1+\theta x) \bmod {\mathfrak{p}_p}^{n-1}$ pour un certain $r \in \{0,\ldots,p-1\}$, ce qui équivaut à la condition $v_p(l-\zeta^r) \geq \frac{n-1}{p-1}$.
Or on remarque que si $1 \leq r \leq p-1$, alors $l - \zeta^r = (l-1) + (1-\zeta^r)$, et $1-\zeta^r$ étant de valuation $\frac{1}{p-1}$, on en déduit que $v_p(l-\zeta^r) = v_p(l-1)$. Donc la condition nécessaire et suffisante précédente se réécrit $v_p(l-1) \geq \frac{n-1}{p-1}$. Alors, en prenant $n > p$, cette condition n'est pas vérifiée quand p divise exactement $l-1$. Or le théorème de la progression arithmétique assure qu'il existe une infinité de nombres premiers l tels que $v_p(l-1) = 1$, et donc pour tous ces nombres l, $v_p(l-\zeta^r) < \frac{n-1}{p-1}$ pour tout $r \in \{0,\ldots,p-1\}$, ce qui assure qu'il y

a bien une infinité de nombres premiers l pour lesquels on n'a pas la propriété de relèvement.

□ □

En particulier, les contrexemples élémentaires de la proposition 3.1 assurent que l'on ne peut pas espérer que la flèche $H^1(F,G) \to H^1(F,G^{\mathrm{ab}})$ soit surjective pour des familles assez générales de groupes. En revanche, si l'on s'intéresse désormais au sous-groupe de $H^1(F,G^{\mathrm{ab}})$ engendré par l'image de cette flèche (cette image n'est pas nécessairement un sous-groupe), on va montrer que pour certaines familles de groupes finis, ce sous-groupe est $H^1(F,G^{\mathrm{ab}})$ tout entier.

Pour cela, introduisons une définition :

Définition 3.2. *Soit G un groupe fini, $q \in \mathbf{N}^*$. On dira qu'un élément $\overline{b}$ de G^{ab} est q-relevable si $\overline{b}^{q-1} = 1$ et il existe $b \in G$ relevant $\overline{b}$ tel que b^q soit conjugué à b.*

À l'aide de cette définition, on est en mesure de donner une caractérisation algébrique du sous-groupe engendré par l'image de $H^1(F,G) \to H^1(F,G^{\mathrm{ab}})$:

Lemme 3.3. *Soit G un groupe fini, F un corps p-adique, q le cardinal du corps résiduel de F. On suppose que $(q,\#G) = 1$. On note $I(G)$ le sous-groupe de $H^1(F,G^{\mathrm{ab}})$ engendré par l'image de la flèche $H^1(F,G) \to H^1(F,G^{\mathrm{ab}})$.*
Alors $I(G)$ est le sous-groupe de $H^1(F,G^{\mathrm{ab}})$ engendré par les morphismes continus $\overline{\phi} : \Gamma_0 \to G^{\mathrm{ab}}$, tels que $\overline{\phi}(\tau)$ est q-relevable.

Démonstration : On a une inclusion évidente de $I(G)$ dans le sous-groupe décrit dans le lemme 3.3, que l'on notera $J(G)$. Soit $\overline{\phi} : \Gamma_0 \to G^{\mathrm{ab}}$ dans $J(G)$. On note $\overline{a} := \overline{\phi}(\sigma)$ et $\overline{b} := \overline{\phi}(\tau)$. Par définition, $\overline{b}$ s'écrit $\overline{b}_1 \dots \overline{b}_r$, avec $\overline{b}_i$ q-relevable. Définissons alors les morphismes $\overline{\phi}_i : \Gamma_0 \to G^{\mathrm{ab}}$ par $\overline{\phi}_i(\sigma) := \overline{a}_i$ et $\overline{\phi}_i(\tau) := \overline{b}_i$, où $a_i \in G$ est un élément tel que $b_i^q = a_i b_i {a_i}^{-1}$, b_i étant un relevé de $\overline{b}_i$ dans G. Définissons aussi $\overline{\psi} : \Gamma_0 \to G^{\mathrm{ab}}$ par $\overline{\psi}(\sigma) := \overline{a}{\overline{a}_1}^{-1} \dots {\overline{a}_r}^{-1}$ et $\overline{\psi}(\tau) := 1$. Alors $\overline{\phi} = \overline{\psi}\overline{\phi}_1 \dots \overline{\phi}_r$ dans le groupe $H^1(F,G^{\mathrm{ab}})$. Or les $\overline{\phi}_i$ se relèvent, i.e. sont dans $I(G)$, et $\overline{\psi}$ aussi, puisqu'il suffit alors de relever $\overline{a}{\overline{a}_1}^{-1} \dots {\overline{a}_r}^{-1}$ dans G de façon quelconque. Donc finalement $\overline{\phi} \in I(G)$, d'où le lemme. □ □

Corollaire 3.4. *Avec les notations précédentes, $I(G) = H^1(F,G^{\mathrm{ab}})$ si et seulement si le sous-groupe ${}_{q-1}G^{\mathrm{ab}}$ des éléments de G^{ab} d'ordre divisant $q-1$ est engendré par les éléments q-relevables.*

Remarquons également le résultat suivant :

Lemme 3.5. *Si G (resp. H) est un groupe fini pour lequel le sous-groupe de $H^1(F,G^{\mathrm{ab}})$ (resp. $H^1(F,H^{\mathrm{ab}})$) engendré par l'image de $H^1(F,G) \to H^1(F,G^{\mathrm{ab}})$ (resp. $H^1(F,H) \to H^1(F,H^{\mathrm{ab}})$) est $H^1(F,G^{\mathrm{ab}})$ (resp. $H^1(F,H^{\mathrm{ab}})$) tout entier, alors le groupe $G \times H$ vérifie également cette propriété.*

Pour montrer cela, il suffit de remarquer que $(G \times H)^{\mathrm{ab}} \cong G^{\mathrm{ab}} \times H^{\mathrm{ab}}$.

Une autre conséquence immédiate est le fait suivant :

Corollaire 3.6. *Soit G un groupe fini. Si $\exp(G)$ divise $q-1$, alors $I(G) = H^1(F, G^{\mathrm{ab}})$.*

En effet, dans ce cas, tout relèvement d'un élément quelconque de G^{ab} est un q-relèvement.

4 Cas des groupes de type ECF

On va s'intéresser dans cette section aux p-groupes constants : on va montrer au théorème 4.3 qu'une certaine famille de p-groupes (de type ECF) vérifie la propriété du corollaire 3.4, mais que ce n'est pas le cas pour un p-groupe général (voir le contrexemple à la fin de cette section). Introduisons pour cela quelques notions de la théorie des p-groupes finis (pour plus de précisions, on pourra consulter [16]) :

Soit G un p-groupe fini. On notera $P_2 := [G,G]$ le groupe dérivé de G, et $P_i := [G, P_{i-1}]$ pour $i \geq 3$. On note $m \geq 2$ l'entier minimal tel que $P_m = 1$. On remarque d'abord que le cas $m = 2$ correspond au cas où G est abélien, pour lequel la surjectivité de $H^1(k,G) \to H^1(k, G^{\mathrm{ab}})$ est évidente. On définit aussi, pour $r = 2, \dots, m-2$, $K_r := \mathrm{Centr}_G(P_r/P_{r+2})$ le centralisateur de P_r/P_{r+2} dans G. Si tous les quotients successifs P_r/P_{r+1} sont d'ordre p, on remarque aisément que les K_r sont des sous-groupes maximaux (i.e. de cardinal p^{n-1}) de G : en effet, on a un morphisme de groupes $G \to \mathrm{Aut}(P_r/P_{r+2})$ de noyau exactement K_r, d'où une injection $G/K_r \hookrightarrow \mathrm{Aut}(P_r/P_{r+2})$. Or P_r/P_{r+2} est un groupe d'ordre p^2, donc un p-Sylow de $\mathrm{Aut}(P_r/P_{r+2})$ est d'ordre p, donc G/K_r est d'ordre au plus p (car il a pour ordre une puissance de p), et ce groupe est non-trivial (sinon $G = K_r$, ce qui implique que $P_{r+1} = P_{r+2}$, ce qui est exclu), donc d'ordre p. Enfin, on notera $P_1 := K_2$.

On peut alors montrer un résultat concernant le sous-groupe engendré par l'image de $H^1(k,G) \to H^1(k, G^{\mathrm{ab}})$, pour une classe de p-groupes G.

Définition 4.1. *Soit G un p-groupe. G est dit de type CF (resp. ECF) si pour tout $2 \leq r \leq m-1$, P_r/P_{r+1} est d'ordre p (resp. P_r/P_{r+1} est d'ordre p et G^{ab} est un groupe abélien élémentaire, i.e. d'exposant p, ce qui équivaut à dire que G^{ab} est un produit de $\mathbf{Z}/p\mathbf{Z}$).*

On dispose alors du théorème suivant (voir par exemple [17], théorèmes A et B) :

Théorème 4.2 (Mac Kay)**.** *Soit G un p-groupe de type CF.*
Alors G admet au plus 3 centralisateurs K_i distincts, et au plus deux tels centralisateurs si $p = 2$.

En appliquant ce théorème et en utilisant les résultats précédents, on va montrer :

Théorème 4.3. *Soit p un nombre premier. Soit G un p-groupe fini de type ECF. Soit l un nombre premier distinct de p. Soit F un corps l-adique.*
Si $p = 2$, on suppose que tous les centralisateurs K_r de G sont égaux, et si $p = 3$, que G admet au plus deux centralisateurs K_r distincts.
Alors le sous-groupe $I(G)$ de $H^1(F, G^{\mathrm{ab}})$ engendré par l'image de $H^1(F, G) \to H^1(F, G^{\mathrm{ab}})$ est $H^1(F, G^{\mathrm{ab}})$ tout entier.

Remarque 4.4.
1. Le théorème reste vrai pour des produits de tels groupes de type ECF, grâce au lemme 3.5.
2. Tous les groupes de type ECF connus ont au plus deux centralisateurs.
3. Les groupes suivants sont des groupes de type ECF qui vérifient les hypothèses du théorème :
   – Les p-groupes de type ECF de degré de commutativité strictement positif (i.e. tel que $[P_i, P_j] \subset P_{i+j+1}$ pour $i, j \geq 1$) : dans ce cas, tous les centralisateurs K_r sont égaux.
   – Les 2-groupes de classe de nilpotence maximale, à savoir les groupes diédraux, semi-diédraux et quaternioniques d'ordre 2^n (voir section 8 pour la définition des groupes de quaternions généralisés). En effet, ces groupes sont de type ECF et de degré de commutativité strictement positif.
   – Les p-groupes de classe de nilpotence maximale, pour $p > 3$.
   – Les groupes de la proposition 3.1.

Corollaire 4.5. *Si G vérifie les hypothèses du théorème 4.3, et si $G \to SL_n$ est un plongement, et k un corps de nombres, notant $X := SL_n/G$, on a l'égalité* $\mathrm{Br}_{\mathrm{nr}_1}(X) = Б_\omega(X) = \mathrm{Br}\ k$.

Démonstration : La seule chose qu'il reste à démontrer est la trivialité de $Ш^1_\omega(k, M)$, et il s'agit juste de remarquer que l'on n'est pas dans un cas spécial (voir [1], chapitre 10, théorème 1) puisque $pM = 0$. □ □

Remarque 4.6. Ce résultat va impliquer dans de nombreux cas que le groupe $\mathrm{Br}_{\mathrm{nr}}(X)$ est trivial (i.e. réduit à Br k). En effet, $\mathrm{Br}_{\mathrm{nr}_1}(X)$ est trivial, et la formule de Bogomolov (voir [6], théorème 7.1) permet de montrer que dans de nombreux cas, $\mathrm{Br}_{\mathrm{nr}}(\overline{X}) = 0$, ce qui assure alors que $\mathrm{Br}_{\mathrm{nr}}(X)$ est trivial. Par exemple, on obtient que pour le groupe diédral d'ordre 2^n, le groupe de Brauer non-ramifié de la variété X est trivial. De même, si G est le groupe quaternionique d'ordre 2^n, le groupe de Brauer non-ramifié de X est trivial (alors que l'on sait que pour le groupe quaternionique d'ordre 16, la variété X n'est pas rationnelle : voir [8], théorème 34.7).

Démonstration : (du théorème 4.3)
Montrons d'abord le lemme crucial suivant :

Lemme 4.7. *Soit G un groupe de type CF, tel que $m > 3$.*
Soit $t \in G \setminus \cup_{r=2}^{m-2} K_r$. Soit $k \in \mathbf{N}^*$.
Si $t^k \in P_2$, alors $t^k \in P_{m-1}$ et il existe un $x \in P_{m-2}$ tel que $t^k = [x, t]$.

Démonstration : Dans toute cette preuve, si H est un sous-groupe de G, $\mathrm{Conj}_H(t)$ désigne la classe de conjugaison de t dans H.

- Montrons d'abord que $t^k \in P_{m-1}$. Si ce n'est pas le cas, alors il existe $2 \leq r \leq m-2$ tel que $t^k \in P_r \setminus P_{r+1}$. Alors le quotient P_r/P_{r+1} est engendré par la classe de t^k, et puisque t commute avec t^k, cela assure que $[t, P_r] \subset P_{r+2}$, i.e. $t \in K_r$, ce qui contredit l'hypothèse. Donc $t^k \in P_{m-1}$.
- On remarque que pour tout $g \in G$, on a $gtg^{-1} = [g, t]\, t$, donc on a l'inclusion $\mathrm{Conj}_G(t) \subset P_2 t$. Or $t \notin K_{m-2}$, donc l'ensemble $\mathrm{Conj}_{P_{m-2}}(t)$ est non-réduit à t, et par conséquent il est de cardinal au moins p (son cardinal est le quotient de celui de P_{m-2} par celui du centralisateur de t dans P_{m-2}, donc un multiple de p). Or on a l'inclusion évidente $\mathrm{Conj}_{P_{m-2}}(t) \subset P_{m-1}t$, et $P_{m-1}t$ est de cardinal exactement p, donc on a en fait l'égalité $P_{m-1}t = \mathrm{Conj}_{P_{m-2}}(t)$. Or on a montré que $t^k \in P_{m-1}$, donc $t^{k+1} \in P_{m-1}t = \mathrm{Conj}_{P_{m-2}}(t)$, ce qui signifie exactement qu'il existe $x \in P_{m-2}$ tel que $t^k = [x, t]$.

□ □

Ce lemme étant acquis, on va maintenant appliquer le théorème de Mac Kay. On notera q le cardinal du corps résiduel de F, qui est une puissance de l. On remarque que ce théorème est évident dans les cas où p ne divise pas $q-1$ (le seul élément de G^{ab} d'ordre divisant $q-1$ est l'élément trivial). Par conséquent, on peut désormais supposer que p divise $q-1$. On note π la projection de G dans G^{ab}, de sorte que l'on dipose d'une suite exacte courte :

$$1 \to P_2 \to G \xrightarrow{\pi} G^{\mathrm{ab}} \to 1$$

1. Supposons d'abord que $m = 3$ (le cas $m = 2$ est trivial, puisqu'alors G est abélien). Alors P_2 est contenu dans le centre de G, il est abélien et d'ordre p. Prenons alors $t \in G \setminus Z(G)$. Alors $\mathrm{Conj}_G(t)$ est non-réduit à t, et contenu dans $P_2 t$ qui est d'ordre p, donc ces deux ensembles sont égaux. On sait donc que tous les éléments de $\pi(G \setminus K)$ sont q-relevables, où $K := Z(G)$.
2. Si $m > 3$, on note $K := \cup_r K_r$. Alors le lemme 4.7 assure que les éléments d'ordre divisant $q-1$ dans $\pi(G \setminus K) \subset G^{\mathrm{ab}}$ sont q-relevables.
3. Montrons alors le lemme suivant :

   Lemme 4.8. *Soit G un groupe de type CF. Si $p = 2$, on suppose que tous les centralisateurs K_r de G sont égaux, et si $p = 3$, que G admet au plus deux centralisateurs K_r distincts. Si $m = 3$, on note $K = Z(G)$, et si $m > 3$, on note $K := \cup_r K_r$.*
   Alors, $G \setminus K$ engendre le groupe G.

Démonstration : Si $m = 3$, $K = Z(G)$ étant un sous-groupe strict de G, G est engendré par $G \setminus K$ (on fixe $t \notin K$, et alors si $g \in K$, g s'écrit $t^{-1}(tg)$, avec t^{-1} et tg dans $G \setminus K$).

Si $m > 3$, par le théorème de Mac Kay, on peut écrire $K = K^{(1)} \cup K^{(2)} \cup K^{(3)}$, avec les $K^{(i)}$ choisis parmi les K_r.

- Si les $K^{(i)}$ sont égaux, i.e. si G n'a qu'un seul centralisateur (par exemple si G est de degré de commutativité strictement positif, i.e. $[P_i, P_j] \subset P_{i+j+1}$), alors $G \setminus K$ engendre G pour toutes les valeurs de p, y compris 2 et 3.
- Dans le cas général, le sous-groupe engendré par $G \setminus K$ contient $G \setminus K$, donc est de cardinal strictement supérieur à $p^n - 3p^{n-1}$ (ce sous-groupe contient le neutre de G), donc strictement supérieur à $p^{n-1}(p-3)$ (à $p^{n-1}(p-2)$ dans le cas où on a seulement deux centralisateurs). Donc dès que $p > 3$, ce cardinal est strictement supérieur à p^{n-1}, et donc le sous-groupe engendré est G tout entier (et si G ne possède que deux centralisateurs distincts, le résultat est valable pour $p = 3$). Finalement, dans tous les cas envisagés, le sous-groupe engendré par $G \setminus K$ est G tout entier.

□ □

4. Montrons enfin le théorème 4.3 : le sous-groupe de G^{ab} engendré par les éléments de ${}_{q-1}G^{\mathrm{ab}} = G^{\mathrm{ab}}$ (car p divise $q-1$ et G^{ab} est d'exposant p) qui sont q-relevables est égal à G^{ab} tout entier : en effet, les éléments de $\pi(G \setminus K)$ sont q-relevables, et par le lemme, $G \setminus K$ engendre G, donc $\pi(G \setminus K)$ engendre G^{ab}. Donc par le corollaire 3.4, $I(G) = H^1(F, G^{\mathrm{ab}})$, ce qui conclut la preuve.

□ □

En fait, pour un p-groupe de type CF (on ne suppose plus l'abélianisé d'exposant p, il peut être quelconque), cette preuve assure que le sous-groupe de $H^1(F, G^{\mathrm{ab}})$ (F est toujours une extension finie de $\mathbf{Q}_l$) engendré par l'image de $H^1(F, G) \to H^1(F, G^{\mathrm{ab}})$ est $H^1(F, G^{\mathrm{ab}})$ tout entier, dans les cas suivants (pour $l \neq p$) :

- p ne divise pas $q - 1$.
- $\exp(G^{\mathrm{ab}})$ divise $q - 1$.

Cependant, quand p divise $q-1$, mais $\exp(G^{\mathrm{ab}})$ ne divise pas $q-1$ (ce qui représente une infinité de nombres l si le groupe n'est pas de type ECF et si le corps F ne contient pas les racines p-ièmes de l'unité), on ne peut pas conclure par cette méthode.

Exemples : Dans les exemples de la proposition 3.1, pour lesquels l'application $H^1(F, G) \to H^1(F, G^{\mathrm{ab}})$ n'est pas surjective, le théorème 4.3 assure que le sous-groupe engendré par l'image de ladite application est $H^1(F, G^{\mathrm{ab}})$, puisque les groupes considérés dans le lemme sont des p-groupes de classe de nilpotence maximale (i.e. $P_{n-1} \neq 1$ et $P_n = 1$), donc des groupes de type ECF (et on montre même qu'ils ont un seul centralisateur, donc on a le résultat pour tous les nombres premiers p).

Contrexemple pour un p-groupe de type CF sur $\mathbf{Q}$ Construisons désormais un groupe fini (et même un p-groupe de type CF) pour lequel le sous-groupe engendré par l'image de $H^1(k_v, G) \to H^1(k_v, G^{\mathrm{ab}})$ est un sous-groupe strict de $H^1(k_v, G^{\mathrm{ab}})$, pour une infinité de places v, le corps k étant le corps des nombres rationnels $\mathbf{Q}$.

Lemme 4.9. *Soit p un nombre premier. Il existe un p-groupe de type CF (d'ordre p^6) et une infinité de nombres premiers l tels que le sous-groupe engendré par l'image de l'application $H^1(\mathbf{Q}_l, G) \to H^1(\mathbf{Q}_l, G^{\mathrm{ab}})$ n'est pas égal à $H^1(\mathbf{Q}_l, G^{\mathrm{ab}})$.*

Démonstration : On définit G comme le produit semi-direct de deux groupes cycliques d'ordre p^3, notés $\langle x \rangle$ et $\langle y \rangle$, pour l'action de $\langle y \rangle$ sur $\langle x \rangle$ définie par $y.x := x^{1-p^2}$. On peut donner une définition de G par générateurs et relations, à savoir $G = \langle x, y : x^{p^3} = y^{p^3} = 1, [x,y] = x^{p^2} \rangle$.

On a donc immédiatement que $P_2 = \langle x^{p^2} \rangle$ est cyclique d'ordre p. On en déduit que l'abélianisé de G est $G^{\mathrm{ab}} = \left(\langle x \rangle / \langle x^{p^2} \rangle \right) \times \langle y \rangle \cong \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^3\mathbf{Z}$. Par conséquent, G est un groupe de type CF mais pas ECF. En particulier les éléments d'ordre divisant p dans cet abélianisé sont ${}_pG^{\mathrm{ab}} = \left(\langle x^p \rangle / \langle x^{p^2} \rangle \right) \times \langle y^{p^2} \rangle$, et donc si on note ${}_p^{P_2}G$ l'image réciproque de ce sous-groupe par la projection canonique $G \to G^{\mathrm{ab}}$, on en déduit que ${}_p^{P_2}G = \langle x^p \rangle \times \langle y^{p^2} \rangle$, sachant que y agit trivialement sur x^p.

Le centre de G est égal à $Z(G) = \langle x^p \rangle \times \langle y^p \rangle$. Par conséquent, ${}_p^{P_2}G \subset Z(G)$.

Fixons alors q tel que p divise exactement $q-1$. Alors ${}_{q-1}^{P_2}G = {}_p^{P_2} G \subset Z(G)$, et les éléments de $1 \times \langle y^{p^2} \rangle$ sont q-relevables car leurs relevés sont d'ordre divisible par p. En revanche, soit $\overline{b} = (t,s) \in_{q-1} G^{\mathrm{ab}} = \left(\langle x^p \rangle / \langle x^{p^2} \rangle \right) \times \langle y^{p^2} \rangle$ avec t non trivial. Alors on va montrer qu'un tel $\overline{b}$ n'est pas q-relevable. En effet, si c'était le cas, il existerait un relevé b de $\overline{b}$ et un $g \in G$ tels que $b^{q-1} = [b,g]$. Or les calculs précédents assurent que $b \in Z(G)$ puisqu'il est dans ${}_{q-1}^{P_2}G$, donc $[b,g] = 1$, et donc $b^{q-1} = 1$. Mais on voit que les éléments de ${}_{q-1}^{P_2}G$ qui sont d'ordre divisant $q-1$, donc divisant p, sont dans $\langle x^{p^2} \rangle \times \langle y^{p^2} \rangle$, donc le fait que b soit dans ce cas assure que $\overline{b} = (t,s) \in \left(\langle x^{p^2} \rangle / \langle x^{p^2} \rangle \right) \times \langle y^{p^2} \rangle = 1 \times \langle y^{p^2} \rangle$, i.e. que t soit trivial, ce qui est exclu.

Finalement, on a montré que les éléments de ${}_{q-1}G^{\mathrm{ab}} = \left(\langle x^p \rangle / \langle x^{p^2} \rangle \right) \times \langle y^{p^2} \rangle$ qui sont q-relevables forment le sous-groupe strict $1 \times \langle y^{p^2} \rangle$. Par conséquent, le corollaire 3.4 assure que, si p divise exactement $l-1$ (ce qui signifie que p divise $l-1$, mais que p^2 ne divise pas $l-1$), alors le sous-groupe engendré par l'image de la flèche $H^1(\mathbf{Q}_l, G) \to H^1(\mathbf{Q}_l, G^{\mathrm{ab}})$ n'est pas $H^1(\mathbf{Q}_l, G^{\mathrm{ab}})$ tout entier. □ □

Remarque 4.10. On a montré, pour ce groupe G, le fait que : pour un corps de nombres k, le sous-groupe engendré par l'image de la flèche $H^1(k_v, G) \to H^1(k_v, G^{\mathrm{ab}})$ n'est pas $H^1(k_v, G^{\mathrm{ab}})$ tout entier, dès que p divise exactement $q_v - 1$, où q_v désigne le cardinal du corps résiduel de k en la place v. On remarque que l'ensemble des telles places est de densité $\frac{1}{p}$ si $k = \mathbf{Q}$, $1 - \frac{1}{p}$ si $k = \mathbf{Q}(\zeta_p)$.

5 Comparaison des groupes $Б_\omega(X)$ et $\mathbf{Br}_{\mathbf{nr}_1}(X)$

Dans cette partie, on va montrer un résultat d'une autre nature que le précédent : en effet, dans la partie 4, aucune hypothèse n'était faite sur le corps de base, en revanche on imposait des conditions sur la structure du groupe. Ici, au contraire, le résultat est valable pour tous les groupes finis, sous réserve d'une restriction sur les racines de l'unité contenues dans le corps de base. Si k est un corps et n un entier naturel, on notera $\mu_n(k)$ l'ensemble des racines n-ièmes de l'unité contenues dans k, et $\mu(k)$ la réunion des $\mu_n(k)$ pour n parcourant $\mathbf{N}$.

Le résultat principal de cette section est le suivant :

Théorème 5.1. *Soit G un groupe fini constant, k un corps de nombres. On suppose que $(\#\mu(k), \exp(G)) = 1$.*

Alors $\mathrm{Br}_{\mathrm{nr}_1}(X) = Б_\omega(X) = \mathrm{Br}\ k$.

Démonstration : On note n l'exposant de G. On sait que G^{ab} est isomorphe à un produit fini $\prod_i \mathbf{Z}/n_i$. On considère le dual $M \cong \prod_i \mu_{n_i}$ du k-groupe G^{ab}. On définit pour toute place v, $I'_v(G)$ comme étant le sous-groupe de $H^1(k_v, M)$ orthogonal à l'image de $H^1(k_v, G)$ dans $H^1(k_v, G^{\mathrm{ab}})$ pour l'accouplement donné par la dualité locale. Soit alors $\alpha \in H^1(k, M)$ tel que α corresponde à un élément de $\mathrm{Br}_{\mathrm{nr}_1}(X)$ qui n'est pas dans $Б_\omega(X)$, i.e. tel que pour presque toute place v, $\alpha_v \in I'_v(G)$, et $\alpha_v \neq 0$ pour une infinité de places v. On écrira $\alpha = (\alpha_i)$, avec $\alpha_i \in H^1(k, \mu_{n_i})$. Par l'isomorphisme de Kummer $H^1(k, \mu_{n_i}) \cong k^*/(k^*)^{n_i}$, α_i peut être vu comme un élément $a_i \in k^*$ modulo $(k^*)^{n_i}$. Par le corollaire 3.6, et en utilisant le théorème de dualité locale, $I'_v(G) = 0$ dès que $n | q_v - 1$. Donc pour presque toute place v vérifiant cette condition, $\alpha_v = 0$, donc $\alpha_{i,v} = 0$ pour tout i. Or la condition $n | q_v - 1$ équivaut à la condition $k(\zeta_n)/k$ totalement décomposée (voir par exemple [24], IV, paragraphe 4).

Intéressons-nous donc au diagramme suivant d'extensions de corps :

$$\begin{tikzcd}
 & K := k(\zeta_n, \sqrt[n_i]{a_i}) \arrow[dl, no head] \arrow[dr, no head] & \\
k(\sqrt[n_i]{a_i}) \arrow[dr, no head] & & k(\zeta_n) \arrow[dl, no head] \\
 & k &
\end{tikzcd}$$

On sait donc que, à un nombre fini de places près, si $k(\zeta_n)/k$ est totalement décomposée en v, $\alpha_v = 0$ et donc $a_i \in (k_v^*)^{n_i}$ pour tout i, donc d'après le diagramme précédent, l'extension K/k est totalement décomposée. Puisque les extensions K/k et $k(\zeta_n)/k$ sont galoisiennes, et puisqu'à un nombre fini de places près, si v est totalement décomposée dans $k(\zeta_n)/k$, alors v est totalement décomposée dans K/k, en utilisant la proposition 13.9 de [20], on sait que K est une sous-extension de $k(\zeta_n)$, donc on a l'inclusion $k(\sqrt[n_i]{a_i}) \subset k(\zeta_n)$, et ce pour tout i. Par conséquent, l'extension $k(\sqrt[n_i]{a_i})/k$ est une extension abélienne de k, comme sous-extension de l'extension abélienne $k(\zeta_n)/k$. Or par hypothèse, k ne contient pas les racines p-ièmes de l'unité, pour p divisant n, alors l'extension $k(\sqrt[n_i]{a_i})/k$ est nécessairement triviale, puisqu'alors une racine n_i-ième de a_i n'a pas de conjugués distincts d'elle-même dans cette extension. Donc finalement $\alpha = 0$. $\square$ $\square$

Remarque 5.2. Le théorème 5.1 va dans le sens du corollaire 9.3 de [18] et du corollaire 2 de [19] dus à Neukirch, et concernant la propriété d'approximation faible pour les groupes constants vérifiant les hypothèses du théorème 5.1.

6 Un contrexemple à la formule $\mathrm{Br}_{nr_1}(X) = \text{Б}_\omega(X)$

Construisons désormais un contrexemple au théorème 5.1 dans le cas où l'hypothèse de primalité entre le cardinal du groupe et l'ordre du groupe des racines de l'unité n'est pas verifiée. Les résultats principaux de cette section sont les propositions 6.1 et 6.4, où l'on construit un espace homogène X à stabilisateur fini constant pour lequel l'obstruction de Brauer-Manin à l'approximation faible associée au groupe $\text{Б}_\omega(X)$ n'est pas la seule. C'est donc un exemple qui montre la différence avec le cas des espaces homogènes à stabilisateurs connexes ou abéliens, pour lesquels cette obstruction est la seule (voir [4]).

On se donne un nombre premier p ($p = 2$ ou p impair), on prend le corps $k = \mathbf{Q}(\zeta_p)$. On considère le groupe G, donné par la présentation suivante :

$$G := \langle x, y, z : x^{p^2} = y^{p^2} = z^{p^2} = 1; [x, y] = z^p \rangle$$

Un tel groupe existe et est d'ordre p^6 (voir par exemple [13]). On a alors le résultat suivant :

Proposition 6.1. *Si* $k = \mathbf{Q}(\zeta_p)$ *et* $G := \langle x, y, z : x^{p^2} = y^{p^2} = z^{p^2} = 1; [x, y] = z^p\rangle$, *alors*

$$\mathrm{Br}\ k = Б_\omega(X) \subsetneq \mathrm{Br}_{\mathrm{nr}_1}(X)$$

Remarque 6.2. Cet exemple répond notamment à la question posée dans [10], avant la proposition 4 : le groupe $Б_\omega(X)$ peut être strictement contenu dans le groupe $\mathrm{Br}_{\mathrm{nr}_1}(X)$.

Démonstration : Rappelons d'abord que l'extension $k/\mathbf{Q}$ est totalement ramifiée en p, donc il existe une unique place de k (notée v_0) au-dessus de p.

Le centre de G est $Z = \langle x^p, y^p, z\rangle$, son groupe des commutateurs est $P_2 = \langle z^p\rangle \cong \mathbf{Z}/p\mathbf{Z}$, son abélianisé est

$$G^{\mathrm{ab}} = \langle x, y, z\rangle/\langle z^p\rangle \cong \langle x\rangle \times \langle y\rangle \times (\langle z\rangle/\langle z^p\rangle) \cong \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$$

Considérons alors une place v de k telle que p divise exactement $q_v - 1$ (p divise toujours $q_v - 1$ pour v distincte de la place au-dessus de p). Soit alors un élément $\overline{b} = (pr, ps, \epsilon) \in G^{\mathrm{ab}} \cong \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ d'ordre p. Ses relevés dans G sont de la forme $b = x^{pr}y^{ps}z^{\epsilon+pk} \in G$. Alors l'élément b est dans Z, donc $\overline{b}$ est q_v-relevable si et seulement si $b^{q_v-1} = 1$ si et seulement si $b^p = 1$ si et seulement si $z^{p\epsilon} = 1$ si et seulement si $\epsilon \equiv 0 \bmod p$ si et seulement si $\overline{b} \in \langle x^p\rangle \times \langle y^p\rangle \cong p\mathbf{Z}/p^2\mathbf{Z} \times p\mathbf{Z}/p^2\mathbf{Z}$. Par conséquent, le sous-groupe de ${}_pG^{\mathrm{ab}} \cong \mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}$ engendré par les éléments q_v-relevables est exactement le sous-groupe $\mathbf{Z}/p\mathbf{Z}\times\mathbf{Z}/p\mathbf{Z}\times 1$. Par conséquent, le groupe $I_v(G) \subset H^1(k_v, G^{\mathrm{ab}}) = H^1(k_v, \mathbf{Z}/p^2\mathbf{Z}) \times H^1(k_v, \mathbf{Z}/p^2\mathbf{Z}) \times H^1(k_v, \mathbf{Z}/p\mathbf{Z})$ (défini comme le sous-groupe engendré par l'image de $H^1(k_v, G)$ dans $H^1(k_v, G^{\mathrm{ab}})$) est contenu dans le sous-groupe $H^1(k_v, \mathbf{Z}/p^2\mathbf{Z}) \times H^1(k_v, \mathbf{Z}/p^2\mathbf{Z}) \times H^1_{\mathrm{nr}}(k_v, \mathbf{Z}/p\mathbf{Z})$. Prenons alors l'élément $a := (0, 0, \alpha) \in H^1(k, M) = H^1(k, \mu_{p^2}) \times H^1(k, \mu_{p^2}) \times H^1(k, \mu_p)$, où α correspond à la classe de ζ_p dans $k^*/(k^*)^p$, i.e. à l'extension de degré p : $k(\zeta_{p^2})/k$.

Alors, si p^2 divise $q_v - 1$, ζ_{p^2} est contenu dans k_v et donc $a_v = 0$. Si p divise exactement $q_v - 1$, a_v est orthogonal à $I_v(G)$ si et seulement si α_v est orthogonal à l'image (i.e. la projection) de $I_v(G)$ dans $H^1(k_v, \mathbf{Z}/p\mathbf{Z})$, et le raisonnement précédent assure que cette projection est exactement $H^1_{\mathrm{nr}}(k_v, \mathbf{Z}/p\mathbf{Z})$. Or pour tout v distinct de la place v_0 au-dessus de p, α est non-ramifié en v, donc $\alpha_v \in H^1_{\mathrm{nr}}(k_v, \mu_p)$, donc par théorème de dualité locale, α_v est orthogonal à $H^1_{\mathrm{nr}}(k_v, \mathbf{Z}/p\mathbf{Z})$, donc a_v est orthogonal à $I_v(G)$ dès que p divise exactement $q_v - 1$. Finalement, l'élement a ainsi construit est bien orthogonal à $I_v(G)$ en presque toute place v (en toute place $v \neq v_0$ en fait), mais il est non-trivial pour les v telles que p divise exactement $q_v - 1$ (i.e. telles que p divise exactement $l^{p-1} - 1$, l étant le premier en-dessous de v) ; or on voit que de telles places sont en nombre infini par le théorème de la progression arithmétique : elles sont en densité $1 - 1/p > 0$. Donc l'élément a n'est pas dans $\text{Ш}^1_\omega(k, M)$. Il correspond donc bien à un élément de $\mathrm{Br}_{\mathrm{nr}_1}(X)$ qui n'est pas dans $\text{Б}_\omega(X)$. □ □

Remarque 6.3. Pour p premier quelconque, le groupe G considéré ici n'est autre que le produit semi-direct $(\mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z}) \rtimes \mathbf{Z}/p^2\mathbf{Z}$ défini de la façon suivante : si on note x, z et y trois générateurs respectifs des trois groupes cycliques d'ordre p^2 apparaissant dans ce produit, l'action de y sur $\langle x\rangle \times \langle z\rangle = \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z}$ est donnée par : $y.(x, 1) := (x, z^p)$ et $y.(1, z) := (1, z)$.

Montrons désormais que l'on a une inclusion stricte : $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)} \subsetneqq X(k_\Omega)^{\text{Б}_\omega(X)}$.

Proposition 6.4. *Si* $k = \mathbf{Q}(\zeta_p)$ *et* $G := \langle x, y, z : x^{p^2} = y^{p^2} = z^{p^2} = 1; [x, y] = z^p\rangle$, *alors*

$$X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)} \subsetneqq X(k_\Omega)^{\text{Б}_\omega(X)} = X(k_\Omega)$$

En particulier, l'obstruction de Brauer-Manin relative au sous-groupe $\text{Б}_\omega(X)$ *n'est pas suffisante pour expliquer le défaut d'approximation faible sur* X.

Démonstration : On considère à nouveau l'élément $a \in H^1(k, M)$ utilisé dans la preuve de la proposition 6.1. Alors on sait que pour toute place v distincte de la place v_0 au-dessus de p, $a_v \cup [Z]\,(P_v) = 0$ pour tout point $P_v \in X(k_v)$. Par conséquent, $(P_v) \in X(k_\Omega)$ est orthogonal à $a \cup [Z]$ si et seulement si $a_{v_0} \cup [Z]\,(P_{v_0}) = 0$. Montrons désormais le lemme suivant :

Lemme 6.5. $I_{v_0}(G) = H^1(k_{v_0}, G^{\mathrm{ab}})$.

Démonstration : On a besoin d'une présentation du groupe de Galois $G_{k_{v_0}}(p)$ de la p-extension maximale de k_{v_0}. Celle-ci est donnée par le théorème (7.5.9) de [21], et il convient de distinguer deux cas : la description de ce groupe diffère selon que le corps k_{v_0} possède seulement les racines 2-ièmes de l'unité (cas $p = 2$) ou qu'il possède les racines p-ièmes de l'unité avec $p > 2$ (cas p impair).

- Si $p = 2$. Alors $G_{k_{v_0}}(p) = G_{\mathbf{Q}_2}(2)$ est le pro-2-groupe à 3 générateurs x_1, x_2, x_3 avec la relation $x_1^2 x_2^4 [x_2, x_3] = 1$. Par conséquent, la donnée d'un morphisme $\phi_{v_0} : G_{k_{v_0}} \to G^{\mathrm{ab}}$ équivaut à celle d'un triplet $(\overline{g}_1, \overline{g}_2, \overline{g}_3) \in_2 G^{\mathrm{ab}} \times G^{\mathrm{ab}} \times G^{\mathrm{ab}}$ (car G^{ab} est d'exposant 4). Notons E l'ensemble des tels triplets qui se relèvent en un triplet $(g_1, g_2, g_3) \in G \times G \times G$ vérifiant la relation $g_1^2 = [g_2, g_3]$. Cela correspond exactement aux morphismes $\phi_{v_0} : G_{k_{v_0}} \to G^{\mathrm{ab}}$ qui proviennent d'un morphisme $\phi'_{v_0} : G_{k_{v_0}} \to G$. Soient alors $(\overline{g}_1, \overline{g}_2, \overline{g}_3) \in_2 G^{\mathrm{ab}} \times G^{\mathrm{ab}} \times G^{\mathrm{ab}}$, et $(g_1, g_2, g_3) \in G \times G \times G$ des relevés quelconques. Si on a la relation $g_1^2 = [g_2, g_3]$, $(\overline{g}_1, \overline{g}_2, \overline{g}_3) \in E$. Sinon, on a deux cas possibles (on rappelle que $G^{\mathrm{ab}} = \langle x, y, z\rangle/\langle z^2\rangle \cong \langle x\rangle \times \langle y\rangle \times (\langle z\rangle/\langle z^2\rangle) \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et que le sous-groupe dérivé est $\langle z^2\rangle \cong \mathbf{Z}/2$) :

- Soit $g_1^2 = 1$ et $[g_2, g_3] = z^2$. Alors la relation $g_1^2 = [g_2, 1]$ et $1^2 = [1, g_3]$ assurent respectivement que les triplets $(\overline{g}_1, \overline{g}_2, 1)$ et $(1, 1, \overline{g_3})$ sont dans E, et donc $(\overline{g}_1, \overline{g}_2, \overline{g_3})$ est dans le sous-groupe engendré par E.
- Soit $g_1^2 = z^2$ et $[g_2, g_3] = 1$. Alors il existe un couple $g, h \in G$ tel que $[gg_2, hg_3] = z^2$, avec g ou h trivial dès que g_1 ou g_2 n'est pas dans le centre de G. On a donc sous cette hypothèse, $(\overline{g}_1, \overline{gg}_2, \overline{hg_3}) \in E$ et $(1, \overline{g}, \overline{h}) \in E$, donc $(\overline{g}_1, \overline{g}_2, \overline{g_3})$ est dans le sous-groupe engendré par E. Enfin, si g_2 et g_3 sont centraux, alors $[xg_2, yg_3] = z^2$, donc $(\overline{g}_1, \overline{xg}_2, \overline{yg_3}) \in E$, $(1, \overline{g}_2, \overline{y}^{-1}\overline{g_3}^{-1}) \in E$ et $(1, \overline{x}^{-1}\overline{g}_2^{-1}, \overline{g_3}) \in E$, et donc $(\overline{g}_1, \overline{g}_2, \overline{g_3})$ est encore dans le sous-groupe engendré par E, ce qui conclut la preuve du lemme 6.5 dans le cas $p = 2$.

- Si $p > 2$. Alors $G_{k_{v_0}}(p)$ est le pro-p-groupe à $p+1$ générateurs $x_1, \ldots, x_{p+1}$ et une relation :
$$x_1^p\,[x_1, x_2]\,[x_3, x_4] \ldots [x_p, x_{p+1}] = 1$$
On raisonne comme précédemment : on note E l'ensemble des $(p+1)$-uplets $(\overline{g_1}, \ldots, \overline{g}_{p+1}) \in_p G^{\mathrm{ab}} \times G^{\mathrm{ab}} \times \cdots \times G^{\mathrm{ab}}$ qui se relèvent en des $(p+1)$-uplets $(g_1, \ldots, g_{p+1}) \in G \times \cdots \times G$ vérifiant $g_1^p\,[g_1, g_2]\,[g_3, g_4] \ldots [g_p, g_{p+1}] = 1$. Étant donnés $(g_1, \ldots, g_{p+1}) \in G \times \cdots \times G$, tels que $g_1^p\,[g_1, g_2]\,[g_3, g_4] \ldots [g_p, g_{p+1}] = z^{pu}$, relevant un élément de ${}_pG^{\mathrm{ab}} \times G^{\mathrm{ab}} \times \cdots \times G^{\mathrm{ab}}$ et avec $1 \leq u \leq p-1$, on distingue à nouveau les deux cas suivants :
- Si $g_1^p = 1$, alors $(\overline{g_1}, 1, \overline{g_3}, 1, \ldots, \overline{g_p}, 1) \in E$ et $(1, \overline{g_2}, 1, \overline{g_4}, \ldots, 1, \overline{g_{p+1}}) \in E$, donc $(\overline{g_1}, \ldots, \overline{g}_{p+1})$ est dans le sous-groupe engendré par E.
- Sinon, $g_1^p = z^{pa_0} \neq 1$ et $[g_{2i-1}, g_{2i}] = z^{pa_i}$. Si l'un des a_i (pour $1 \leq i \leq \frac{p+1}{2}$) n'est pas divisible par p, alors on remplace par exemple g_{2i} par h_{2i} puissance adéquate de g_{2i}, et on obtient un élément dont le projeté est dans E, et puisque $(1, 1, \ldots, 1, \overline{g_{2i}}\overline{h_{2i}}^{-1}, 1, \ldots, 1) \in E$, $(\overline{g_1}, \ldots, \overline{g}_{p+1})$ est bien dans le sous-groupe engendré par E. Si au contraire, tous les $[g_{2i-1}, g_{2i}]$ sont triviaux, alors on raisonne exactement comme dans le second point du cas $p = 2$, en multipliant les deux dernières composantes g_p et g_{p+1} par des éléments qui ne commutent pas (en distinguant à nouveau le cas où g_p et g_{p+1} sont centraux) et en utilisant la cyclicité de P_2, on trouve aussi que $(\overline{g_1}, \ldots, \overline{g}_{p+1})$ est dans le sous-groupe engendré par E, ce qui termine la preuve du lemme 6.5.

□ □

Terminons maintenant la preuve de la proposition 6.4. On sait donc que $I_{v_0}(G) = H^1(k_{v_0}, G^{\mathrm{ab}})$, et donc $\{[Z]\,(P_{v_0}) : P_{v_0} \in X(k_{v_0})\}$ engendre tout $H^1(k_{v_0}, G^{\mathrm{ab}})$. Or $a_{v_0} \neq 0$, et le cup produit local est non-dégénéré, donc il existe un point P_{v_0} tel que $a_{v_0} \cup [Z]\,(P_{v_0}) \neq 0$, et donc en prenant P_v quelconque pour $v \neq v_0$, on obtient un point $(P_v) \in X(k_\Omega)$ qui n'est pas Brauer-Manin orthogonal à $a \cup [Z] \in \mathrm{Br}_{\mathrm{nr}_1}(X)$. Enfin, on n'est pas dans un "cas spécial" (voir par exemple [1]), donc $Ш^1_\omega(k, M) = 0$, donc $Б_\omega(X) = \mathrm{Br}\, k$, donc il n'y a pas d'obstruction de Brauer-Manin relative à $Б_\omega(X)$. Donc finalement, $(P_v) \in X(k_\Omega)^{Б_\omega(X)} \setminus X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)}$. □ □

Remarque 6.6. Sous les hypothèses de la proposition 6.4, en appliquant le corollaire 2 du lemme 5.3 de [2] et le lemme 5.6 de [2] (appliqué à un facteur minimal du groupe G), et en utilisant le fait que G est d'ordre p^6 et G^{ab} n'est pas annulé par p, on voit que le groupe $\mathrm{Br}_{\mathrm{nr}}(\overline{X})$ est trivial. Par conséquent, dans l'exemple de la proposition 6.4, il n'y a pas d'obstruction transcendante à l'approximation faible, et donc $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)} = X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)}$. Donc par le théorème 1 de [10], on en déduit que $\overline{X(k)} = X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)}$, c'est-à-dire que l'obstruction de Brauer-Manin algébrique à l'approximation faible sur X est bien la seule.

7 Obstruction de Brauer-Manin

L'objectif de cette section est de décrire l'obstruction de Brauer-Manin à l'approximation faible sur les espaces homogènes considérés en termes plus concrets de cohomologie galoisienne des groupes finis (voir théorème 7.1). On est dans la situation suivante : G est un k-groupe fini, k un corps de nombres. On plonge G dans $\mathbf{SL}_{n,k}$, et on considère la k-variété $X := \mathbf{SL}_n/G$. On a un dessin de la forme :

$$\begin{tikzcd}
\mathbf{SL}_n \arrow[dd, "G"'] \arrow[dr, "D(G)"] & \\
& Z \arrow[dl, "G^{\mathrm{ab}}"] \\
X &
\end{tikzcd}$$

L'objectif est d'utiliser une méthode de fibration pour montrer par exemple que l'obstruction de Brauer-Manin à l'approximation faible sur X est la seule. On peut en effet construire une fibration $f : Y \to B$ où Y est k-stablement-birationnel à X et B est un espace homogène d'un $\mathbf{SL}_{m,k}$ à stabilisateur G^{ab} (voir par exemple [10], preuve du théorème 1).

Pour appliquer les méthodes de fibration, on a besoin d'avoir des points locaux dans les fibres de f, ce qui se traduit en terme de cohomologie galoisienne par la situation suivante : on se donne $(P_v) \in X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}}$, S un ensemble fini de places. On note pour toute place v, $\sigma_v := [Z]\,(P_v) \in H^1(k_v, G^{\mathrm{ab}})$. On considérera aussi $H_v(G) := \mathrm{Im}(H^1(k_v, G) \to H^1(k_v, G^{\mathrm{ab}}))$ et $I_v(G)$ le sous-groupe de $H^1(k_v, G^{\mathrm{ab}})$ engendré par $H_v(G)$. La situation idéale est celle où il existe $\alpha \in H^1(k, G^{\mathrm{ab}})$ tel que :

- $\alpha_v = \sigma_v$ pour toute place $v \in S$.
- $\alpha_v \in H_v(G)$ pour toute place v de k.

Cela correspond géométriquement au fait que, étant donnés $(P_v)_{v\in\Omega} \in Y(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1} Y}$, et S un ensemble fini de places de k, il existe $Q \in B(k)$ arbitrairement proche des $f(P_v)$ pour v dans S, de sorte que pour toute place v de k (pas seulement sur S), la fibre $f^{-1}(Q_v)$ admet un k_v-point, i.e. la fibre $f^{-1}(Q)$ a des points dans tous les complétés de k.

On va montrer un résultat proche de cette situation idéale, mais néanmoins différent, à savoir qu'il existe $\alpha \in H^1(k, G^{\mathrm{ab}})$ tel que :

– $\alpha_v = \sigma_v$ pour toute place $v \in S$.

– $\alpha_v \in I_v(G)$ pour toute place v de k.

Le résultat principal de cette section généralise en quelque sorte le théorème 4 de [10], en considérant non plus l'obstruction associée au sous-groupe $Б_\omega(X)$, mais celle associée au sous-groupe $\mathrm{Br}_{\mathrm{nr}_1}(X)$, dont on a vu à la proposition 6.4 qu'elles pouvaient être différentes. Pour cela, on définit $H^1_I(k, G^{\mathrm{ab}})$ comme l'ensemble des éléments de $H^1(k, G^{\mathrm{ab}})$ dont la localisation en v est dans $I_v(G)$ pour toute place v hors de k.

Théorème 7.1. *Soit G un k-groupe fini. Alors on a équivalence entre :*

1. $\overline{X(k)} = X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}}$.
2. *Pour tout ensemble fini de places S, l'image de l'application $H^1(k, G) \to \prod_{v\in S} H^1(k_v, G)$ est constituée des éléments $(g_v)_{v\in S}$ dont l'image $(g'_v)_{v\in S}$ dans $\prod_{v\in S} H^1(k_v, G^{\mathrm{ab}})$ provient de $H^1_I(k, G^{\mathrm{ab}})$.*

Remarque 7.2. On voit donc que l'obstruction de Brauer-Manin ne semble pas distinguer l'image $H_v(G)$ de $H^1(k_v, G) \to H^1(k_v, G^{\mathrm{ab}})$ du sous-groupe $I_v(G)$ engendré par cette image. Or en général, $H_v(G)$ est strictement plus petit que $I_v(G)$. Une idée pour construire un espace homogène X pour lequel l'obstruction de Brauer-Manin n'est pas la seule, pourrait donc être la suivante : trouver un groupe G pour lequel l'obstruction de Brauer-Manin disparait (par exemple un groupe de type ECF), et construire des classes locales $\sigma_v \in H_v(G)$ pour $v \in S$ de sorte que pour tout élément $\alpha \in H^1(k, G^{\mathrm{ab}})$ relevant ces classes locales, il existe une place v' telle que $\alpha_{v'} \notin H_{v'}(G)$. En effet, si l'obstruction de Brauer-Manin disparaît, les résultats précédents assurent que l'application $H^1_I(k, G^{\mathrm{ab}}) \to \prod_{v\in S} H_v(G)$ est surjective. Or si X vérifie l'approximation faible, l'application $H^1_H(k, G^{\mathrm{ab}}) \to \prod_{v\in S} H_v(G)$ doit être surjective ($H^1_H(k, G^{\mathrm{ab}})$ est l'ensemble des éléments de $H^1(k, G^{\mathrm{ab}})$ qui sont localement partout dans $H_v(G)$). Or $H^1_H(k, G^{\mathrm{ab}})$ est a-priori plus petit que $H^1_I(k, G^{\mathrm{ab}})$, donc peut-être est-il possible que la première flèche soit surjective, mais pas la seconde.

Plus généralement, ce théorème est une conséquence du résultat suivant, qui est lui-même une conséquence de la suite exacte de Poitou-Tate et qui est un analogue du théorème 4.4 de [18] :

Proposition 7.3. *Soit M un Γ_k-module fini, M' son dual. Soit S un ensemble fini de places de k, contenant les places où le module M est ramifié. On se donne pour toute place v hors de S un sous-groupe I_v de $H^1(k_v, M)$ contenant $H^1_{\mathrm{nr}}(k_v, M)$. On notera I'_v l'orthogonal de I_v pour le cup-produit local. On définit $H^1_{I,S}(k, M)$ (resp. $H^1_{I',S}(k, M')$) comme l'ensemble des éléments de $H^1(k, M)$ (resp. $H^1(k, M')$) dont la localisation en v est dans I_v (resp. I'_v) pour toute place v hors de S.*

On a alors une suite exacte de groupes abéliens :

$$H^1_{I,S}(k, M) \to \prod_{v \in S} H^1(k_v, M) \to H^1_{I',S}(k, M')^D$$

où la dernière flèche est donnée par la somme des cup-produits locaux.

Démonstration : Il est clair que cette suite est un complexe : en effet, soit $\alpha \in H^1_{I,S}(k, M)$. Montrons que l'image φ de α dans $H^1_{I',S}(k, M')^D$ est nulle. Pour cela, on se donne $\beta \in H^1_{I',S}(k, M')$, et on calcule $\varphi(\beta) = \sum_{v \in S} \alpha_v \cup \beta_v$. Or pour toute place $v \notin S$, $\alpha_v \cup \beta_v = 0$ par définition de $H^1_{I,S}(k, M)$ et de $H^1_{I',S}(k, M')$, donc $\varphi(\beta) = \sum_{v \in \Omega_k} \alpha_v \cup \beta_v = 0$ car α et β sont des éléments globaux et la suite de Poitou-Tate (voir [21], 8.6.10) est un complexe.

Il reste donc à vérifier l'exactitude au centre. On considère le diagramme commutatif suivant :

$$\begin{tikzcd}
H^1_{I,S}(k, M) \arrow[r] \arrow[d, "i"] & \prod'_{v \notin S} I_v \times \prod_{v \in S} H^1(k_v, M) \arrow[r, "d_S"] \arrow[d] & H^1_{I',S}(k, M')^D \\
H^1(k, M) \arrow[r] & \prod'_{v \in \Omega_k} H^1(k_v, M) \arrow[r, "d"] & H^1(k, M')^D \arrow[u, "i'^*"']
\end{tikzcd}$$

où $\prod'_{v \notin S} I_v$ est le produit restreint des I_v par rapport aux $H^1_{\mathrm{nr}}(k_v, M)$, et $\prod'_{v \in \Omega_k} H^1(k_v, M)$ le produit restreint des $H^1(k_v, M)$ par rapport aux $H^1_{\mathrm{nr}}(k_v, M)$.

On sait que la seconde ligne de ce diagramme est exacte (elle est extraite de la suite exacte de Poitou-Tate : voir [21], 8.6.10). Soit $(\alpha_v)_{v \in S} \in \prod_{v \in S} H^1(k_v, M)$ tel que $d_S((\alpha_v)) = 0$. On note (α'_v) l'image de (α_v) dans $\prod'_{v \in \Omega_k} H^1(k_v, M)$ via l'injection naturelle $\prod_{v \in S} H^1(k_v, M) \to \prod'_{v \in \Omega_k} H^1(k_v, M)$, et $\delta := d((\alpha'_v)) \in H^1(k, M')^D$. Par construction, $i'^*(\delta) = 0$. Or le noyau de i'^* est le dual de $\prod'_{v \notin S} H^1(k_v, M')/I'_v$ (produit restreint pour les sous-groupes $H^1_{\mathrm{nr}}(k_v, M')/I'_v$), et ce dual s'identifie par dualité locale à $\prod'_{v \notin S} I_v$. Donc δ correspond à un élément $(\beta_v) \in \prod'_{v \notin S} I_v$. Définissons alors l'élément $\gamma_v := \alpha_v$ si $v \in S$ et $\gamma_v := -\beta_v$ si $v \notin S$. Alors $(\gamma_v) \in \prod'_{v \notin S} I_v \times \prod_{v \in S} H^1(k_v, M)$, et par construction il a une image nulle dans $H^1(k, M')^D$, donc il se relève en un élément global γ^0 dans $H^1(k, M)$ (par exactitude de la seconde ligne du diagramme), et par construction cet élément est bien dans $H^1_{I,S}(k, M)$, ce qui conclut la preuve. □ □

Remarque 7.4. Si on pose $\Lambda := \prod'_{v \notin S} I_v$, sous-groupe ouvert de $\prod'_v H^1(k_v, M)$, d'orthogonal $\Lambda^\perp = \prod_{v \in S} H^1(k_v, M) \times \prod_{v \notin S} I'_v(G)$ dans $\prod'_v H^1(k_v, M')$, et si on note $\rho : H^1(k, M) \to \prod'_v H^1(k_v, M)/\Lambda$, on définit comme Neukirch (cf [18], 4.3), les groupes $\triangle(k, M, \Lambda) := \mathrm{Coker}(\rho)$ et $\triangledown(k, M', \Lambda^\perp) := \mathrm{Ker}(\rho)/Ш^1(k, M')$, alors la dualité locale induit une dualité parfaite de groupes finis (voir [18], théorème 4.4) :

$$\triangle(k, M, \Lambda) \times \triangledown(k, M', \Lambda^\perp) \to \mathbf{Q}/\mathbf{Z}$$

qui traduit exactement l'exactitude de la suite de la proposition.

Une conséquence de ce résultat est une interprétation de l'obstruction de Brauer-Manin pour un k-groupe fini quelconque (pas forcément constant) :

Corollaire 7.5. *Soit G un groupe algébrique fini sur k, $X := \mathbf{SL}_n/G$ pour un plongement $G \to \mathbf{SL}_{n,k}$. Pour toute place v de k, on note $I_v(G)$ le sous-groupe de $H^1(k_v, G^{\mathrm{ab}})$ engendré par l'image $H_v(G)$ de l'application $H^1(k_v, G) \to H^1(k_v, G^{\mathrm{ab}})$. Soit $(P_v) \in X(k_\Omega)$. On a alors la caractérisation suivante :*

$(P_v) \in X(k_\Omega)^{\mathrm{Br_{nr_1}}}$ si et seulement si $([Z](P_v))_{v \in \Omega}$ est dans l'adhérence de $H^1(k, G^{\mathrm{ab}})$ dans le produit restreint $\prod'(H^1(k_v, G^{\mathrm{ab}}) : I_v(G))$.

Remarque 7.6. On sait que la condition $(P_v) \in \overline{X(k)}$ implique que $([Z](P_v))_{v \in \Omega}$ est dans l'adhérence de $H^1(k, G^{\mathrm{ab}})$ dans le produit restreint $\prod'(H^1(k_v, G^{\mathrm{ab}}) : H_v(G))$ ($H_v(G)$ n'est pas un sous-groupe de $H^1(k_v, G^{\mathrm{ab}})$, mais cela permet tout de même de définir une topologie produit restreint).

On peut reformuler ce résultat à la manière du théorème 4 de [10] et obtenir ainsi le théorème 7.1 : *Démonstration* : *(du théorème 7.1)*

- On suppose que l'assertion 1. est vérifiée.
  Soit S un ensemble fini de places de k. Soit $(g_v)_{v \in S} \in \prod_{v \in S} H^1(k_v, G)$, d'images respectives g'_v dans $H^1(k_v, G^{\mathrm{ab}})$, tels qu'il existe $g^0 \in H^1_I(k, G^{\mathrm{ab}})$ vérifiant $g^0_v = g'_v$ pour toute place v dans S. Pour montrer la propritété 2., il suffit de trouver $(P_v) \in X(k_\Omega)^{\mathrm{Br_{nr_1}}(X)}$ tel que $[Y](P_v) = g_v$ pour v dans S. Le groupe $\mathrm{Br_{nr_1}}(X)/\mathrm{Br}\, k$ est fini (puisque X est unirationnelle), on peut donc trouver un ensemble de représentants fini $E = \{e_1, \dots, e_n\}$ de ce quotient dans $\mathrm{Br_{nr_1}}(X)$, de sorte que tout élément $e_i \in E$ s'écrive $e_i = a_i \cup [Z]$ pour un élément a_i dans $H^1(k, M)$, orthogonal à $I_v(G)$ en presque toute place v. Quitte à augmenter S, on peut supposer que pour toute place v hors de S, et pour tout i, $a_{i,v}$ est orthogonal à $I_v(G)$.
  Le torseur $\mathbf{SL}_n \to X$ étant versel, il existe $P_v \in X(k_v)$ tel que $[\mathbf{SL}_n](P_v) = g_v \in H^1(k_v, G)$. Pour toute place v hors de S, on choisit un point $P_v \in X(k_v)$ arbitraire. Ainsi en toute place v, $[Z](P_v)$ est dans $I_v(G)$ (c'est l'image de $[\mathbf{SL}_n](P_v)$). Fixons un entier i, et calculons $\sum_{v \in \Omega_k} j_v(e_i(P_v))$. On remarque que pour toute place $v \in S$, $e_i(P_v) = a_{i,v} \cup [Z](P_v) = a_{i,v} \cup g^0_v$. Or si $v \notin S$,

$a_{i,v} \cup [Z]\,(P_v) = 0$ car $a_{i,v}$ est orthogonal à $I_v(G)$, et $a_{i,v} \cup g_v^0 = 0$ car $a_{i,v}$ est orthogonal à $I_v(G)$ et $g_v^0 \in I_v(G)$. Donc on a

$$\sum_{v \in \Omega_k} j_v(e_i(P_v)) = \sum_{v \in \Omega_k} j_v(a_{i,v} \cup [Z]\,(P_v)) = \sum_{v \in \Omega_k} j_v(a_{i,v} \cup g_v^0) = 0$$

par loi de réciprocité globale, car $a_i \cup g^0 \in \mathrm{Br}\, k$. On a donc bien construit $(P_v) \in X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)}$ vérifiant $[\mathbf{SL}_n]\,(P_v) = g_v$ pour toute place v de S. On conclut alors en approchant $(P_v)_{v \in S}$ par un point rationnel $m \in X(k)$ (par l'assertion 1.), et l'élément $\tilde{g} := [\mathbf{SL}_n]\,(m) \in H^1(k, G)$ s'envoie bien sur $(g_v)_{v \in S}$ dans $\prod_{v \in S} H^1(k_v, G)$, d'où l'assertion 2.

– On suppose désormais la propriété 2. vérifiée.
On se donne $(P_v) \in X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}_1}(X)}$. Soit S un ensemble fini de places de k. Par le théorème 7.3, appliqué pour les sous-groupes $I_v := I_v(G)$, on dispose de la suite exacte suivante :

$$H^1_{I,S}(k, G^{\mathrm{ab}}) \to \prod_{v \in S} H^1(k_v, G^{\mathrm{ab}}) \to H^1_{I',S}(k, M)^D$$

Par hypothèse, $([Z]\,(P_v))_{v \in S} \in \prod_{v \in S} H^1(k_v, G^{\mathrm{ab}})$ est envoyé sur 0 dans $H^1_{I',S}(k, M)^D$, puisque pour $a \in H^1_{I',S}(k, M)$, $\sum_{v \in S} j_v(a_v \cup [Z]\,(P_v)) = \sum_{v \in \Omega_k} j_v(a_v \cup [Z]\,(P_v)) = 0$ par la propriété de Brauer-Manin (pour la première égalité, on remarque simplement que pour $v \notin S$, $[Z]\,(P_v) \in I_v(G)$ et a_v est orthogonal à $I_v(G)$). Donc par exactitude, l'élément $([Z]\,(P_v))_{v \in S}$ provient d'un élément de $H^1_{I,S}(k, G^{\mathrm{ab}})$. Donc par la propriété 2., l'élément $([Y]\,(P_v))_{v \in S} \in \prod_{v \in S} H^1(k_v, G)$ provient d'un élément de $H^1(k, G)$. Cela assure qu'il existe un cocyle $g \in Z^1(k, G)$ tel que le torseur tordu $f^g : (\mathbf{SL}_n)^g \to X$ admet un k_v-point Q_v au-dessus de P_v, pour $v \in S$. Or $H^1(k, \mathbf{SL}_n) = 0$ (Hilbert 90), donc $(\mathbf{SL}_n)^g$ est isomorphe sur k à $\mathbf{SL}_n$, et donc en particulier $(\mathbf{SL}_n)^g$ vérifie l'approximation faible : il existe $r \in (\mathbf{SL}_n)^g(k)$ arbitrairement proche des Q_v pour $v \in S$. Finalement, le point $m := f^g(r) \in X(k)$ est arbitrairement proche des P_v, pour $v \in S$. Cela assure que la propriété 1. est vérifiée.

□ □

8 Approximation faible pour le groupe Q_{16} sur $\mathbf{Q}$

Définition 8.1. *On dit qu'un k-groupe fini G vérifie l'approximation faible sur k si la variété $X := \mathbf{SL}_n/G$ définie grâce à un plongement $G \to \mathbf{SL}_{n,k}$ vérifie l'approximation faible sur k.*

Dans cette section, on montre que le groupe des quaternions d'ordre 16, noté Q_{16}, vérifie l'approximation faible sur $\mathbf{Q}$. On rappelle d'abord la définition des groupes de quaternions généralisés : si $n \geq 2$, on note Q_{2^n} le groupe des quaternions d'ordre 2^n, défini par exemple par générateurs et relations :

$$Q_{2^n} := \langle a, b : a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, ba = a^{-1}b \rangle$$

L'une des motivations pour l'étude des groupes de quaternions généralisés est la suivante : on sait que la variété $X_n = \mathbf{SL}_m / Q_{2^n}$ est rationnelle (et donc vérifie l'approximation faible) pour $n = 2$ et $n = 3$, et non-rationnelle pour $n = 4$ (voir par exemple [8], théorème 34.7). En outre, le corollaire 4.5 et la remarque qui suit assurent que le groupe de Brauer non-ramifié de la variété X_n est trivial pour tout n. Il n'y a donc pas d'obstruction de Brauer-Manin à l'approximation faible sur X_n. En outre, la variété X_n ($n \geq 3$) n'entre pas dans le cadre des résultats de [10].

Avant de se lancer dans la preuve, on décrit $H_l(Q_{16}) \subset H^1(\mathbf{Q}_l, Q_{16}^{\mathrm{ab}})$ selon les valeurs de l. Pour tout $l \neq 2$, $\epsilon \in \mathbf{Q}_l^*$ désigne une unité qui n'est pas un carré dans $\mathbf{Q}_l$. On rappelle quand dans ce cas, le groupe $H^1(\mathbf{Q}_l, \mathbf{Z}/2) = \mathbf{Q}_l^* / (\mathbf{Q}_l^*)^2$ est formé des classes de $1, \epsilon, l, \epsilon l$ modulo $(\mathbf{Q}_l^*)^2$. un élément de $H^1(\mathbf{Q}_l, \mathbf{Q}_{16}^{\mathrm{ab}})$ sera ainsi décrit par un couple (d_1, d_2), où $d_i \in \{1, \epsilon, l, \epsilon l\}$. On a alors la description suivante de l'ensemble des éléments de $H_l(Q_{16})$:

$l \equiv 1 \bmod 8$		$l \equiv 3$ ou $5 \bmod 8$		$l \equiv 7 \bmod 8$	
d_1	d_2	d_1	d_2	d_1	d_2
1	1	1	1	1	1
1	ϵ	1	ϵ	1	ϵ
1	l				
1	ϵl				
ϵ	1	ϵ	1	ϵ	1
ϵ	ϵ	ϵ	ϵ	ϵ	ϵ
				ϵ	l
				ϵ	ϵl
l	1	l	1	l	1
l	l	l	l	l	l
ϵl	1	ϵl	1	ϵl	1
ϵl	ϵl	ϵl	ϵl	ϵl	ϵl

Montrons le lemme suivant, qui sera utile pour le calcul de l'obstruction de Brauer-Manin dans les fibres.

Lemme 8.2. *Soit* G *une* $\mathbf{Q}$*-forme de* $\mathbf{Z}/4$*. Soit* M *le* $\Gamma_{\mathbf{Q}}$*-module dual.*
Alors $Ш^1_\omega(\mathbf{Q}, M) = 0$.

Démonstration : Si G est $\mathbf{Q}$-isomorphe à $\mathbf{Z}/4$, alors le résultat est bien connu. Sinon, le groupe G est vu comme un $\mathrm{Gal}(L|\mathbf{Q})$-module cyclique d'ordre 4, où $L/\mathbf{Q}$ est une extension quadratique, le générateur σ du groupe de Galois agissant sur le générateur de $\mathbf{Z}/4$ par multiplication par -1. Par conséquent, on vérifie que G s'intègre dans une suite exacte de $\Gamma_{\mathbf{Q}}$-modules :

$$0 \to \mathbf{Z}/4 \xrightarrow{\mathrm{N}} \mathbf{Z}/4\,[L/\mathbf{Q}] \to G \to 0$$

où $\mathbf{Z}/4[L/\mathbf{Q}]$ est le $\mathrm{Gal}(L|\mathbf{Q})$-module isomorphe comme groupe abélien à $\mathbf{Z}/4 \oplus \mathbf{Z}/4$, muni de l'action de σ qui échange les deux composantes, et N est la norme (i.e. l'application diagonale). Par conséquent, le dual M de G apparaît dans la suite exacte suivante :

$$0 \to M \to \mathbf{R}_{L/\mathbf{Q}}(\mu_4) \xrightarrow{N_{L/\mathbf{Q}}} \mu_4 \to 0$$

On considère alors les suites exactes longues de cohomologie :

$$\begin{tikzcd}
\mu_4(L) \arrow[r, "N_{L/\mathbf{Q}}"] \arrow[d] & \mu_4(\mathbf{Q}) \arrow[r] \arrow[d] & H^1(\mathbf{Q}, M) \arrow[r] \arrow[d] & L^*/L^{*4} \arrow[r, "N_{L/\mathbf{Q}}"] \arrow[d] & \mathbf{Q}^*/\mathbf{Q}^{*4} \arrow[d] \\
\prod_v \mu_4(L_v) \arrow[r] & \prod_l \mu_4(\mathbf{Q}_l) \arrow[r] & \prod_l H^1(\mathbf{Q}_l, M) \arrow[r] & \prod_v L_v^*/L_v^{*4} \arrow[r] & \prod_l \mathbf{Q}_l^*/\mathbf{Q}_l^{*4}
\end{tikzcd}$$

Deux cas se présentent alors :

- Si $i \in L$. Alors l'application $H^0(\mathbf{Q}, \mathbf{R}_{L/\mathbf{Q}}(\mu_4)) \xrightarrow{N_{L/\mathbf{Q}}} H^0(\mathbf{Q}, \mu_4)$ est le morphisme trivial $\mu_4(L) = \{\pm 1, \pm i\} \xrightarrow{N_{L/\mathbf{Q}}} \{\pm 1\}$.
- Si $i \notin L$. Alors l'application $H^0(\mathbf{Q}, \mathbf{R}_{L/\mathbf{Q}}(\mu_4)) \xrightarrow{N_{L/\mathbf{Q}}} H^0(\mathbf{Q}, \mu_4)$ est le morphisme trivial $\mu_4(L) = \{\pm 1\} \xrightarrow{(.)^2} \{\pm 1\}$.

Donc dans les deux cas, on a un diagramme commutatif à lignes exactes :

$$\begin{tikzcd}
0 \arrow[r] & \mu_4(\mathbf{Q}) \arrow[r] \arrow[d] & H^1(\mathbf{Q}, M) \arrow[r] \arrow[d] & L^*/L^{*4} \arrow[r, "N_{L/\mathbf{Q}}"] \arrow[d] & \mathbf{Q}^*/\mathbf{Q}^{*4} \arrow[d] \\
\prod_v \mu_4(L_v) \arrow[r] & \prod_l \mu_4(\mathbf{Q}_l) \arrow[r] & \prod_l H^1(\mathbf{Q}_l, M) \arrow[r] & \prod_v L_v^*/L_v^{*4} \arrow[r] & \prod_l \mathbf{Q}_l^*/\mathbf{Q}_l^{*4}
\end{tikzcd}$$

Soit alors $\alpha \in Ш^1_\omega(\mathbf{Q}, M)$. Son image dans L^*/L^{*4} est triviale localement presque partout, donc elle est triviale globalement (on n'est pas dans un cas spécial), donc α provient d'un élément β de $\mu_4(\mathbf{Q})$. Si α est non-trivial, $\beta = -1$. Puisque β_l se relève dans $\mu_4(L_v)$ pour presque toute place l, on a $-1 \in \mathrm{Im}(\prod_{v|l} \mu_4(L_v) \xrightarrow{N_{L_v/\mathbf{Q}_l}} \mu_4(\mathbf{Q}_l))$. Cela assure que pour presque toute place de $\mathbf{Q}$, soit $L/\mathbf{Q}$ est totalement décomposée, soit $\mathbf{Q}(i)/\mathbf{Q}$ l'est. Notons $L = \mathbf{Q}(\sqrt{d})$. Si $\mathbf{Q}(\sqrt{-d})/\mathbf{Q}$ est totalement décomposée en

l, alors $L/\mathbf{Q}$ ou $\mathbf{Q}(i)/\mathbf{Q}$ l'est aussi, donc les deux le sont. Donc $\mathbf{Q}(\sqrt{-d})$ contient à la fois L et $\mathbf{Q}(i)$, donc $d = 1$, cas qui avait été exclu au départ. Donc α est trivial. □□

Avant de montrer le résultat proprement dit, montrons le critère suivant, qui dit en quelque sorte qu'il suffit de travailler au niveau de l'abélianisé :

Lemme 8.3. *On note $H^1_H(k, Q_{16}^{\mathrm{ab}})$ l'ensemble des éléments de $H^1(k, Q_{16}^{\mathrm{ab}})$ qui sont localement partout dans $H_l(Q_{16})$. Alors : Q_{16} vérifie l'approximation faible sur $\mathbf{Q}$ si et seulement si pour tout ensemble fini de places S, l'application $H^1_H(\mathbf{Q}, Q_{16}^{\mathrm{ab}}) \to \prod_{l \in S} H_l(Q_{16})$ est surjective.*

Démonstration : C'est essentiellement une conséquence du lemme précédent, couplée à une méthode de fibration. En effet, soit $(\alpha_v)_{v\in S} \in \prod_{v\in S} H_v(Q_{16})$ (provenant des éléments $a_v \in H^1(\mathbf{Q}_v, Q_{16})$ que l'on veut approcher). On suppose que ces (α_v) sont l'image d'un élèment $\alpha^0 \in H^1_H(\mathbf{Q}, Q_{16}^{\mathrm{ab}})$. Alors l'élément α^0 provient d'un élément $\beta^0 \in H^1(\mathbf{Q}, Q_{16})$: en effet, en termes géométriques, et en utilisant les notations de [10], preuve du théorème 1, on est dans la situation suivante : on construit un morphisme $f : Z \to B$, où Z est stablement k-birationnel à X, et B est un espace homogène d'un groupe semi-simple simplement connexe à stabilisateur Q_{16}^{ab}, et on dispose de points locaux $(P_v)_{v\in S} \prod_{v\in S} Z(k_v)$ (correspondant aux a_v) d'images respectives $Q_v := f(P_v) \in B(k_v)$ (correspondant aux α_v). Dans ce cas, la fibre de f au-dessus d'un point Q^0 approchant les Q_v, et correspondant à α^0, sera un espace homogène de $\mathbf{SL}_n$ à stabilisateur cyclique d'ordre 4, avec des points locaux en toute place de $\mathbf{Q}$ (puisque $\alpha^0 \in H^1_H(\mathbf{Q}, Q_{16}^{\mathrm{ab}})$). Or l'obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible est la seule sur un tel espace, et par le lemme 8.2, le groupe de Brauer de la fibre est trivial, donc cette obstruction disparaît et la fibre va donc vérifier le principe de Hasse et l'approximation faible. Enfin, par le théorème des fonctions implicites, on peut bien approcher les points initiaux de $Z(k_v)$ (correspondants aux a_v) par un point rationnel, ce qui conclut la preuve. □□

Théorème 8.4. *Le groupe Q_{16} vérifie l'approximation faible sur* $\mathbf{Q}$.

Démonstration : On va utiliser le critère du lemme 8.3. Soit S un ensemble fini de places contenant la place infinie, mais ne contenant pas 2. On note $S' := S \cup \{2\}$. On se donne des données locales $\alpha_l \in H_l(Q_{16}) \subset H^1(\mathbf{Q}_l, Q_{16}^{\mathrm{ab}})$ pour toute place $l \in S'$. Chaque élément α_l, $l \in S$, correspond à un couple $d_1^l, d_2^l \in \mathbf{Q}_l^*/\mathbf{Q}_l^{*2}$.

1. On note S_1 l'ensemble des places $l \in S$ telles que l'élément d_1^l soit ramifié, S_2 celui des places $l \in S$ telles que l'élément d_2^l soit ramifié. Notons alors $\delta_i := \prod_{l \in S_i} l$, pour $i = 1, 2$.
2. Quitte à ajouter un nombre fini de places à S_1 et S_2, et quitte à multiplier δ_1, δ_2 par 2, on peut supposer que δ_1 et δ_2 réalisent la condition locale en 2 (en

effet, une telle condition est définie par des congruences modulo 8 ou 16 pour les d_i : par exemple, $\delta_1 \equiv -1 \bmod 8$ et $\delta_2 \equiv 10 \bmod 16$).

3. On pose, pour $\{i,j\} = \{1,2\}$, $\pi_i := \prod_{l \in S_i} \left(\frac{d'^l_j}{l}\right)$, où d'_j est par définition égal à d_j/l si l divise d_j, et à d_j sinon. Quitte à ajouter une place $l_1 \equiv 1 \bmod 8$ dans S_1 et une place $l_2 \equiv 1 \bmod 8$ dans S_2, ainsi que des conditions locales (dans $H_{l_i}(Q_{16})$) bien choisies en ces deux places, on peut supposer que $\pi_1 = \pi_2 = 1$ (voir théorème 111 de [12] ainsi que la description explicite de $H_l(Q_{16})$ dans le cas $l \equiv 1 \bmod 8$).
4. On pose $\pi'_i := \prod_{l \in S_i} \left(\frac{\delta'^l_j}{l}\right)$. Si $\pi'_1 = -1$, on ajoute une place l_1 à S_1 telle que $\left(\frac{\delta_2}{l_1}\right) = -1$, $l_1 \equiv 1 \bmod 8$ et on pose $\alpha_{l_1} = (l_1, 1)$ avec les identifications précédentes. De même, si $\pi'_2 = -1$, on ajoute une place l_2 à S_2 telle que $\left(\frac{\delta_1}{l_2}\right) = -1$, $l_2 \equiv 1 \bmod 8$ et on pose $\alpha_{l_2} = (1, l_2)$. On peut alors supposer que $\pi'_1 = \pi'_2 = \pi_1 = \pi_2 = 1$.
5. En utilisant à nouveau le théorème 111 de [12], on sait qu'il existe un nombre premier $p \equiv 1 \bmod 8$ de sorte que $p \notin S$ et $\left(\frac{\delta'_1 p}{l}\right) = \left(\frac{d'^{\,l}_1}{l}\right)$ pour tout $l \in S$. Alors on a $\left(\frac{\delta_2}{p}\right) = \prod_{l \in S_2} \left(\frac{l}{p}\right) = \prod_{l \in S_2} \left(\frac{p}{l}\right)$, or $\prod_{l \in S_2} \left(\frac{\delta'_1 p}{l}\right) = \pi_2 = 1$ et $\prod_{v \in S_2} \left(\frac{\delta'_1}{l}\right) = \pi'_2 = 1$, donc $\left(\frac{\delta_2}{p}\right) = 1$.
6. De même, il existe $q \neq p$, $q \notin S$, $q \equiv 1 \bmod 8$ tel que $\left(\frac{\delta'_2 q}{l}\right) = \left(\frac{d'^{\,l}_2}{l}\right)$ pour tout $l \in S$ et $\left(\frac{p}{q}\right) = 1$. Alors on vérifie immédiatement que $\left(\frac{\delta_1}{q}\right) = 1$.
7. On considère alors $D_1 := \delta_1 p$ et $D_2 := \delta_2 q$. Alors l'élement $\alpha^0 := (D_1, D_2) \in H^1(\mathbf{Q}, \mathbf{Z}/2 \times \mathbf{Z}/2)$ vérifie :
   - $\alpha^0_l = \alpha_l$ pour tout $l \in S'$.
   - $\alpha^0_l \in H_l(Q_{16})$ pour tout $l \notin S' \cup \{p, q\}$.
   - en la place p (resp. q), $\alpha^0_p = (p.r, 1)$ (resp. $\alpha^0_q = (1, q.r')$), donc grâce à la description explicite de $H_p(Q_{16})$ (resp. $H_q(Q_{16})$), on sait que $\alpha^0_p \in H_p(Q_{16})$ (resp. $\alpha^0_q \in H_q(Q_{16})$).
8. Finalement, cela assure que $\alpha^0 \in H^1_H(\mathbf{Q}, Q^{\mathrm{ab}}_{16})$ et $\alpha^0_l = \alpha_l$ pour tout $l \in S'$, et cela conclut la preuve grâce au lemme 8.3.

□ □

Remarque 8.5. Pour le cas général des groupes Q_{2^n}, $n \geq 5$, le lemme 8.2 n'est plus valable lorsque l'on remplace $\mathbf{Z}/4$ par $\mathbf{Z}/2^{n-2}$, avec $n \geq 5$ (en effet, on sait que $Ш^1_\omega(\mathbf{Q}, \mu_8) \neq 0$ par exemple). Cependant, grâce à la proposition 10 de [22], page I.31, et à l'analogue de la preuve du théorème 8.4, on sait que l'on peut faire la première étape d'une méthode de fibration : étant donnés $(\alpha_l)_{l\in S} \in \prod_{l\in S} H_l(Q_{2^n})$, il existe $\alpha^0 \in H^1(\mathbf{Q}, Q_{2^n}^{\mathrm{ab}})$ se relevant dans $H^1(\mathbf{Q}, Q_{2^n})$ et tel que $\alpha_v^0 = \alpha_v$ pour toute place v de S. Cependant, pour l'étape suivante (approximation faible dans les fibres de la fibration), on a a priori une obstruction de Brauer-Manin à l'approximation faible dans les fibres, puisque le lemme 8.2 n'est plus valable. On est en fait dans une situation de fibres multiples, où la méthode de fibration ne s'applique pas, sauf si les fibres vérifient l'approximation faible (ce qui est le cas pour Q_{16}).

Remerciements Je remercie chaleureusement David Harari pour son soutien et ses nombreux commentaires sur ce travail.

Références

[1] Emil Artin and John Tate, *Class field theory*, second ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1990.

[2] F. A. Bogomolov, *The Brauer group of quotient spaces of linear representations*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 3, 485–516, 688.

[3] Mikhail Borovoi, *Abelianization of the second nonabelian Galois cohomology*, Duke Math. J. **72** (1993), no. 1, 217–239.

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

[5] Jean-Louis Colliot-Thélène and Boris È. Kunyavskiĭ, *Groupe de Picard et groupe de Brauer des compactifications lisses d'espaces homogènes*, J. Algebraic Geom. **15** (2006), no. 4, 733–752.

[6] 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)*, Algebraic groups and homogeneous spaces, Tata Inst. Fund. Res. Stud. Math., Tata Inst. Fund. Res., Mumbai, 2007, pp. 113–186.

[7] Yuval Z. Flicker, Claus Scheiderer, and Ramdorai Sujatha, *Grothendieck's theorem on non-abelian H^2 and local-global principles*, J. Amer. Math. Soc. **11** (1998), no. 3, 731–750.

[8] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003.

[9] David Harari, *Méthode des fibrations et obstruction de Manin*, Duke Math. J. **75** (1994), no. 1, 221–260.

[10] ———, *Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini*, Bull. Soc. Math. France **135** (2007), no. 4, 549–564.

[11] David Harari and Alexei N. Skorobogatov, *Non-abelian cohomology and rational points*, Compositio Math. **130** (2002), no. 3, 241–273.

[12] David Hilbert, *The theory of algebraic number fields*, Springer-Verlag, Berlin, 1998, Translated from the German and with a preface by Iain T. Adamson, With an introduction by Franz Lemmermeyer and Norbert Schappacher.

[13] Rodney James, *The groups of order p^6 (p an odd prime)*, Math. Comp. **34** (1980), no. 150, 613–637.

[14] Martin Kneser, *Galois-Kohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern. I*, Math. Z. **88** (1965), 40–47.

[15] ———, *Galois-Kohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern. II*, Math. Z. **89** (1965), 250–272.

[16] C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, London Mathematical Society Monographs. New Series, vol. 27, Oxford University Press, Oxford, 2002, Oxford Science Publications.

[17] Susan McKay, *On the structure of a special class of p-groups. II*, Quart. J. Math. Oxford Ser. (2) **41** (1990), no. 164, 431–448.

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

[19] ———, *On solvable number fields*, Invent. Math. **53** (1979), no. 2, 135–164.

[20] ———, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[21] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[22] Bernadette Riou-Perrin, *Plongement d'une extension diédrale dans une extension diédrale ou quaternionienne*, Publications Mathématiques d'Orsay 79 [Mathematical Publications of Orsay 79], vol. 4, Université de Paris-Sud Département de Mathématique, Orsay, 1979.

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

[24] Jean-Pierre Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[25] ______, *Cohomologie galoisienne*, fifth ed., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994.

[26] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001.

Cyril Demarche
Laboratoire de Mathématiques, Bâtiment 425, Université de Paris-Sud, F-91405 Orsay, France
Tel. : +033-1 69 15 57 82
email : cyril.demarche@math.u-psud.fr