# Une invitation à la cohomologie galoisienne

Introduction au Domaine de Recherche

Louis Mallet-Burgues

11 septembre 2025

## Table des matières



## Abstract

On introduit l'outil de la cohomologie galoisienne via l'exemple des algèbres centrales simples sur un corps et du groupe de Brauer, puis on donne quelques résultats importants et quelques exemples d'utilisation de cette théorie. On parle ensuite de dimension cohomologique et des propriétés $C_i$ des corps et on explique les liens entre ces deux notions d'apparences très différentes. On termine en évoquant la conjecture de Kato et Kuzumaki qui raffine les conditions $C_i$ pour tenter d'avoir une vraie caractérisation diophantienne de la dimension cohomologique des corps.

# Introduction

La cohomologie galoisienne est un outil essentiel en théorie des nombres et en géométrie arithmétique, qui unifie des questions de nature arithmétique assez diverses. L'idée de base est la suivante : si $k$ est un corps, disons parfait pour simplifier, de clôture algébrique $\overline{k}$, on dispose du groupe de Galois absolu $G_k = \mathrm{Aut}_k(\overline{k})$ qui est muni d'une certaine topologie du fait qu'il peut s'obtenir comme limite des groupes finis $\mathrm{Gal}(\ell/k)$ avec $\ell//k$ extension finie de $k$. On peut alors associer une théorie cohomologique à ce groupe $G_k$ : pour tout groupe abélien $A$ muni d'une action de $G_k$, on associe des groupes abéliens de cohomologie $H^n(k, A)$ qui ont de bonnes propriétés fonctorielles en $k$ et en $A$.
Typiquement, on pourra prendre $A = \overline{k}^\times$ ou $A = \mu_n$ (les racines $n$-èmes de l'unité de $\overline{k}$). Ces groupes ont parfois des interprétations assez diverses, par exemple $H^1(k, \mu_n) \cong k^\times/(k^\times)^n$ si $n$ est premier à la caractéristique de $k$, ou encore $H^2(k, \overline{k}^\times)$ qui classifie les algèbres à division centrales sur $k$ à équivalence de Brauer près.
On introduit la cohomologie galoisienne par l'exemple fondamental des algèbres centrales simples (CSA) sur un corps $k$, que l'on décrit comme des *formes tordues* d'algèbres de matrices, qui sont classifiées par de la cohomologie. L'exemple de base dont le lecteur a probablement entendu parler est celui de l'algèbre des quaternions de Hamilton, $\mathbb{H}$, qui est une $\mathbb{R}$-algèbre non-commutative de dimension 4 engendrée par deux éléments $i$ et $j$ de carré $-1$ qui vérifient $(ij)^2 = -1$ et $ji = -ij$. Cette algèbre n'est pas isomorphe à $M_2(\mathbb{R})$, mais si l'on essaie de définir la même algèbre en partant de $\mathbb{C}$ comme corps de base, on obtient l'algèbre $M_2(\mathbb{C})$. On dit que $\mathbb{H}$ se déploye sur le corps $\mathbb{C}$ et cela peut se traduire par des propriétés cohomologiques liées aux groupes de Brauer de $\mathbb{R}$ et $\mathbb{C}$ qui classifient les algèbres à division sur $\mathbb{R}$ et $\mathbb{C}$.

À partir de la cohomologie de $k$, il est possible de définir une notion de dimension cohomologique. Moralement, un corps $k$ est de dimension cohomologique au plus $i$ si les groupes $H^n(k, A)$ sont tous nuls pour $n > i$. La notion de dimension cohomologique se comporte vraiment comme une dimension, au sens où par exemple le corps $\mathbb{C}(x, y, z)$ est de dimension cohomologique 3, et le corps $\mathbb{C}((T))$ est de dimension cohomologique 1.

De façon surprenante, il semble possible de chercher des conditions diophantiennes sur le corps $k$ pour contrôler sa dimension cohomologique. Par exemple on montre que certains corps, dits $C_1$, ont un groupe de Brauer nul (c'est le cas des corps finis), ce qui implique qu'ils sont de dimension cohomologique au plus 1. On peut aussi introduire plus généralement les propriétés $C_i$ qui sont des conditions diophantiennes sur les corps définies par l'existence de solutions à des équations polynomiales homogènes avec beaucoup plus de variables que le degré (i.e. $n > d^i$ avec $n$ le nombre de variables et $d$ le degré). Il existe alors de nombreuses similarités entre les propriétés $C_i$ et "dimension cohomologique au plus $i$" mais pour autant les deux conditions ne sont pas équivalentes.

La conjecture de Kato et Kuzumaki que j'ai étudiée pendant mon stage sous la direction de Diego Izquierdo tente de raffiner la condition $C_i$ afin d'obtenir une propriété diophantienne équivalente à la propriété "dimension cohomologique au plus $i$". Cette nouvelle condition fait intervenir d'autres invariants du corps $k$, appelés groupes de $K$-théorie de Milnor de $k$. Encore une fois, cette conjecture dans toute sa généralité est fausse mais il existe des résultats positifs dans des cas de la vie de tous les jours.

Dans tout le document, on ne travaille qu'avec des corps *parfaits* pour simplifier l'exposition, bien que la théorie s'adapte avec quelques efforts supplémentaires en remplaçant les clôtures algébriques par des clôtures séparables.

# 1 Algèbres à division et algèbres centrales simples

## 1.1 Définitions et exemples

Une question qui motive la cohomologie galoisienne est celle de la classification des algèbres à division centrales sur un corps $k$. Une algèbre à division sur $k$ est une $k$-algèbre (non-nécessairement commutative) de dimension finie non-nulle dans lequel tout élément non-nul est inversible. Autrement dit, on prend la définition d'extension de corps et on enlève la condition de non-commutativité. Pour exclure le cas simple des extensions de corps, qui est déjà traité par la théorie de Galois, on ajoute la condition que le centre des algèbres qui nous intéressent soit $k$ : on parle alors de $k$-algèbre à division *centrale*. Pour certains corps, il est assez facile de classifier ces algèbres.

**Proposition 1.1.1.** *Si $k$ est un corps algébriquement clos, alors la seule $k$-algèbre à division centrale est $k$ lui-même.*
*Pour ce qui est du corps $\mathbb{R}$ qui n'est pas bien loin d'être algébriquement clos, les seules algèbres à division centrales sur $\mathbb{R}$ sont, à isomorphisme près, $\mathbb{R}$ et $\mathbb{H}$ l'algèbre des quaternions.*

*Démonstration.* Soit $D$ une $k$-algèbre à division centrale avec $k$ algébriquement clos. Alors pour tout $x \in D$, $k[x]$ est un corps car $D$ est de dimension finie et à division, et c'est donc une extension finie de $k$, ce qui force $k[x] = k$ puisque $k$ est algébriquement clos. On a donc $D = k$.
Soit maintenant $D$ une $\mathbb{R}$-algèbre à division centrale, qui n'est pas isomorphe à $\mathbb{R}$. En considérant un élément $a \in D \setminus \mathbb{R}$, on construit une extension finie non-triviale de $\mathbb{R}$, $\mathbb{R}(a)$, qui est isomorphe à $\mathbb{C}$. On en déduit l'existence d'un élément $i \in D$ tel que $i^2 = -1$. On montre alors facilement par analyse-synthèse que :

$$D = C(i) \oplus AC(i)$$

avec $C(i)$ le commutant de $i$, c'est à dire l'espace des éléments qui commutent à $i$, et $AC(i)$ l'espace des éléments qui anti-commutent à $i$, au sens où $xi = -ix$.
Ensuite, on montre que $C(i) = \mathbb{R}[i]$ car $\mathbb{R}[i]$ est algébriquement clos et donc ne possède pas d'extension non-triviale. Enfin, on montre que $AC(i)$ est un $C(i)$-espace vectoriel de dimension 1 puisque si $x, y \in AC(i)$ sont non-nuls, alors $x^{-1}y \in C(i)$. On en déduit que $D$ est de dimension 4, puis il est facile de construire un élément $j \in AC(i)$ de carré $-1$ et d'en déduire que $D$ est isomorphe à $\mathbb{H}$. □

Un autre cas intéressant est celui des corps finis. On peut en effet montrer que tout corps (non-nécessairement commutatif) fini est en fait commutatif. C'est un théorème de Wedderburn. Pour en donner une démonstration qui va dans le sens des idées de la géométrie arithmétique, il nous faut un petit peu plus de théorie sur les algèbres à division.

## 1.2 Algèbres centrales simples

Ce qui suit est bien plus qu'une définition, c'est un théorème d'algèbre non-commutative.

**Définition 1.2.1.** *Soit $k$ un corps parfait et $\overline{k}$ une clôture algébrique de $k$. Une algèbre centrale simple (CSA) sur un corps (parfait) $k$ est, de façon équivalente :*

- *Une $k$-algèbre de dimension finie qui est à la fois centrale, c'est à dire de centre égal à $k$, et simple, au sens où les seuls idéaux bilatères non-triviaux sont $(0)$ et $(1)$.*
- *Une $k$-algèbre $A$ telle qu'il existe une extension finie $\ell/k$ vérifiant $A \otimes_k \ell \cong M_n(\ell)$ comme $\ell$-algèbres.*

— *Une $k$-algèbre $A$ telle que $A \otimes_k \overline{k} \cong M_n(\overline{k})$ comme $\overline{k}$-algèbres.*

Il est plutôt clair que les algèbres à division centrales sur $k$ sont aussi des CSA sur $k$, et l'avantage des CSA est qu'elles forment une structure plus riche que les algèbres à divisions centrales, comme on le verra plus tard. On remarque tout de suite qu'à cause des définitions 2 et 3, une algèbre à division centrale sur $k$ est toujours de dimension $n^2$ avec $n \geq 1$ un entier appelé le *degré* de l'algèbre. La philosophie à avoir en tête est qu'une CSA est une *forme tordue* de l'algèbre $M_n(k)$. Il est possible de rendre cette idée vague très formelle : une CSA ressemble beaucoup à $M_n(k)$, elle ne devient isomorphe à $M_n(\bullet)$ qu'après extension des scalaires à un corps suffisament grand. D'ailleurs, on dira d'une CSA qu'elle se *déploye* sur $\ell$ si elle devient isomorphe à une algèbre de matrices après extension des scalaires à $\ell$. Par exemple, on peut montrer que l'algèbre des quaternions $\mathbb{H}$ se déploye sur $\mathbb{C}$, c'est à dire qu'on a un isomorphisme de $\mathbb{C}$-algèbres :

$$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$$

ce qui n'est pas étonnant puisque $\mathbb{C}$ est un corps algébriquement clos.

**Remarque 1.2.2.** Pour les géomètres et les topologues, on peut faire une analogie avec la notion de fibré vectoriel. Un fibré vectoriel sur un espace $X$ est un faisceau qui est *localement isomorphe* à un faisceau libre. Ici, une CSA est un objet *localement isomorphe* à une algèbre de matrices, pour une bonne notion de localement qui est possible en remplaçant la notion de faisceau sur un espace topologique par la notion plus générale de faisceau sur un *site de Grothendieck*. Cette analogie se poursuivra quand on classifiera ces formes tordues par un groupe de cohomologie (penser au groupe de Picard qui classifie les fibrés en droite).

## 1.3 Descente galoisienne

Un outil important pour comprendre les formes tordues d'un objet est la théorie de la descente, qui est une philosophie très générale et qui dans notre cas s'appelle la descente galoisienne. L'idée est la suivante : si $k$ est un corps parfait de clôture algébrique $\overline{k}$ et de groupe de Galois absolu $G_k = \mathrm{Gal}(\overline{k}/k)$, on peut établir un dictionnaire entre les objets définis sur $k$ et les objets définis sur $\overline{k}$ munis d'une certaine action de $G_k$. Le cas le plus simple est celui des espaces vectoriels.
Concrètement, si $V$ est un $k$-espace vectoriel, on peut former $V_{\overline{k}} = V \otimes_k \overline{k}$ qui est un $\overline{k}$-espace vectoriel muni d'une action de $G_k$ qui vérifie la propriété suivante : pour tout $x \in V_{\overline{k}}$, $\sigma \in G_k$ et $\lambda \in \overline{k}$, on a :

$$\sigma(\lambda x) = \sigma(\lambda)\sigma(x).$$

On dit alors que $V_{\overline{k}}$ est un $\overline{k}$-espace vectoriel avec une action compatible de $G_k$. Dans l'autre sens, si $W$ est un $\overline{k}$-espace vectoriel avec action compatible de $G_k$, on peut prendre les points fixes $W^{G_k}$ de l'action et obtenir un $k$-espace vectoriel. On obtient alors une équivalence de catégories :

$$\{k - \text{espaces vectoriels}\} \simeq \{\overline{k} - \text{espaces vectoriels avec une action compatible de } G_k\}$$

via $V \mapsto V_{\overline{k}}$ et $W \mapsto W^{G_k}$.
On parle alors de *descente galoisienne* car on peut descendre un objet défini sur $\overline{k}$ en un objet défini sur $k$. Il existe de nombreuses généralisations de cette idée, par exemple on peut munir $V$ d'une donnée supplémentaire, comme un tenseur (par exemple une structure d'algèbre) et on demande alors que le tenseur soit compatible avec l'action de $G_k$ pour préserver l'équivalence de catégories.

On va tout de suite appliquer cette idée pour construire les norme et trace réduites des algèbres centrales simples.

## 1.4 Norme et trace réduites

Puisque une CSA ressemble à une algèbre de matrice, on peut définir un déterminant et une trace, appelés norme et trace réduites. Concrètement, si $A$ est une CSA, on se donne un isomorphisme :

$$A \otimes_k \overline{k} \xrightarrow{f} M_n(\overline{k})$$

et on considère la composée $\overline{N} = \det \circ f : A \otimes_k \overline{k} \longrightarrow \overline{k}$, et de même avec la trace. On montre alors que cette application "descend" en une application $N : A \longrightarrow k$ par un argument de descente galoisienne. Détaillons cela : le groupe de Galois absolu $G_k = \mathrm{Aut}_k(\overline{k})$ agit à la fois sur $A \otimes_k \overline{k}$ et sur $\overline{k}$, et $\overline{N}$ est équivariante pour cette action, au sens où pour tout $\sigma \in G_k$ et tout $x \in A \otimes_k \overline{k}$, on a :

$$N(\sigma x) = \sigma N(x).$$

Ceci est dû au fait que les seuls automorphismes d'algèbre de $M_n(\overline{k})$ viennent de la conjugaison par une matrice et le déterminant (et la trace) sont invariants par conjugaison. Ceci permet donc de définir deux applications :

$$A \longrightarrow k$$

de trace et norme, notée $N$ et Tr, qui sont même des *fonctions polynomiales* homogènes, à $n^2$ variables, et de degrés respectifs $n$ et 1.
De plus, l'application $N$ est multiplicative et on en déduit que si $D$ est une algèbre à division, le seul 0 non-trivial de $N$ est 0. Cette observation couplée au théorème de Chevalley-Warning suivant assure que toute algèbre à division finie est un corps (commutatif).

**Théorème 1.4.1.** *Soit $k$ un corps fini de caractéristique $p$ et $f$ une fonction polynomiale à $m$ variables de degré $d$ avec $m > d$. Alors le nombre de zéros de $f$ est divisible par $p$. En particulier, $f$ possède un 0 non-trivial.*

*Démonstration.* Donnons rapidement une idée de preuve car c'est très joli. On note $V \subseteq k^m$ l'ensemble des zéros de $f$ et on considère $\chi$, la fonction indicatrice de $V$, que l'on peut écrire ainsi avec $q = |k|$ :

$$\chi(x) = 1 - f(x)^{q-1}$$

et on calcule alors dans le corps $k$ :

$$|V| = \sum_{x \in k^m} \chi(x)$$

via des formules bien connues de sommes de polynômes sur les corps finis, pour obtenir 0 à cause des restrictions sur le degré de $f$. □

On en déduit le théorème de Wedderburn.

**Théorème 1.4.2.** *Toute algèbre à division finie est un corps (commutatif).*

Plus généralement, notre preuve montre que pour tout corps dans lequel la seconde partie du théorème de Chevalley-Warning est valable (à partir de "En particulier"), il n'y a qu'une seule algèbre à division centrale à isomorphisme près. Ces corps sont appelés $C_1$, et il existe une notion de corps $C^i$ pour tout $i$ comme on le verra ensuite.

# 2 Cohomologie galoisienne

On rappelle que si $k$ est un corps parfait, son groupe de Galois absolu est le groupe *profini* $G_k = \mathrm{Gal}(\overline{k}/k)$ muni de la topologie de Krull, pour laquelle deux éléments $\sigma$ et $\tau$ sont proches s'ils coincident sur une grande extension de $k$. Un tel groupe profini possède une théorie cohomologique dont nous allons à présent dire quelques mots, en partant de l'étude des CSA sur $k$.

## 2.1 Classification des CSA par des cocycles

Soit $k$ un corps parfait et $A$ une CSA sur $k$. On fixe un isomorphisme de $\overline{k}$-algèbres :

$$M_n(\overline{k}) \xrightarrow{\varphi} A \otimes_k \overline{k}.$$

Chaque membre de cet isomorphisme est muni d'une action du groupe $G_k$, mais $\varphi$ n'a pas de raison d'être compatible à cette action. En effet, $\varphi$ est compatible à cette action si et seulement si l'isomorphisme descend en un isomorphisme de $k$-algèbres entre $A$ et $M_n(k)$ par un argument de descente galoisienne. On comprend alors qu'on a une information très riche sur $A$ en regardant le défaut de compatibilité de $\varphi$ à l'action de $G_k$, que l'on peut définir comme ceci :
Pour tout $\sigma \in G_k$, on définit $c_\sigma \in \mathrm{Aut}(M_n(\overline{k}))$ comme la composée suivante :

$$c_\sigma = \varphi^{-1} \circ \sigma \circ \varphi \circ \sigma^{-1}.$$

Il est alors facile de vérifier que l'on a, pour tous $\sigma, \tau \in G_k$ :

$$c_{\sigma\tau} = c_\sigma \circ c_\tau^\sigma$$

où $h^\sigma = \sigma \circ h \circ \sigma^{-1}$.
Une telle donnée est appelée un 1-cocycle et on peut montrer que si $A$ et $B$ sont deux CSA sur $k$ de degré $n$ et si $(\alpha_\sigma)$ et $(\beta_\sigma)$ sont des cocycles associés respectivement à $A$ et $B$, alors $A$ et $B$ sont isomorphes si et seulement si $(\alpha_\sigma)$ et $(\beta_\sigma)$ sont *cohomologues*, au sens où il existe $\theta \in \mathrm{Aut}(M_n(\overline{k}))$ qui vérifie pour tout $\sigma \in G_k$ :

$$\alpha_\sigma = \theta^{-1} \beta_\sigma \theta^\sigma.$$

Ceci amène donc naturellement à la définition suivante.

**Définition 2.1.1.** *(Premier ensemble de cohomologie)*
*Soit $G$ un groupe profini agissant sur un groupe $F$ par automorphismes de groupes. On suppose que l'action est continue lorsque $F$ est muni de la topologie discrète. On définit l'ensemble pointé $H^1(G,F)$ comme l'ensemble des 1-cocyles de $G$ à valeurs dans $F$, c'est à dire les applications continues $c_\bullet : G \longrightarrow F$ qui vérifient la relation de cocycle écrite plus haut, modulo la relation de cohomologie que l'on vient de voir.*
*Le point particulier de cet ensemble pointé est la classe triviale, associée au cocycle qui vaut toujours $1_F$.*

Dans le cas qui nous intéresse, on a $F = \mathrm{Aut}(M_n(\overline{k})) = \mathrm{PGL}_n(\overline{k})$ par le théorème de Skolem-Noether, de sorte que les CSA sur $k$ de degré $n$ sont classifiées à isomorphisme près par l'ensemble :

$$H^1(G_k, \mathrm{PGL}_n(\overline{k})).$$

On a donc trouvé un objet abstrait qui traduit en combinatoire toute la théorie des CSA de degré $n$ sur $k$.

**Remarque 2.1.2.** La puissance de cette idée vient notamment du fait qu'un même ensemble de cohomologie peut classifier des choses très différentes en apparence. Par exemple, en géométrie algébrique, on appelle *variété de Severi-Brauer* une forme tordue de $\mathbb{P}^n_{\overline{k}}$, c'est à dire une variété sur $k$ qui devient isomorphe à $\mathbb{P}^n_{\overline{k}}$ après extension des scalaires à $\overline{k}$. Par la philosophie très générale des formes tordues, celles-ci sont classifiées par l'ensemble :

$$H^1(G_k, \mathrm{Aut}(\mathbb{P}^n_{\overline{k}})) = H^1(G_k, \mathrm{PGL}_{n+1}(\overline{k}))$$

ce qui montre que les variétés de Severi-Brauer de dimension $n$ correspondent à des CSA de degré $n+1$ et réciproquement.

## 2.2 Cohomologie des groupes (profinis)

Dans ce qui suit, le lecteur peut ignorer toutes les considérations topologiques pour une lecture plus simple.
Si nous avons parlé du premier ensemble de cohomologie, c'est qu'il en existe plusieurs. En fait, il est très difficile de concevoir une théorie cohomologique lorsque le groupe $F$ sur lequel agit $G$ est non-commutatif. C'est pourquoi on s'intéresse ici au cas de la cohomologie abélienne. Considérons donc un groupe (profini) $G$ agissant sur un groupe abélien $A$ par automorphismes (avec une action continue). Il existe alors une suite de groupes abéliens :

$$H^n(G, A)$$

que l'on peut définir de façon combinatoire avec des cocycles et des cobords, et qui possède de nombreuses bonnes propriétés fonctorielles, en $G$ et en $A$. Une manière de définir ces groupes est de partir du point de vue abstrait de l'algèbre homologique en considérant le foncteur $A \mapsto A^G$ qui à $A$ associe le groupe abélien des points fixes de $A$ par l'action de $G$, et de dériver à droite ce foncteur exact à gauche. Concrètement, la propriété fondamentale qu'on obtient ainsi est la suivante.

**Proposition 2.2.1.** *Soit $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ une suite exacte courte de G-modules (c'est à dire de groupes abéliens discrets sur lesquels G agit continûment). On a alors une suite exacte longue de groupes abéliens induite par ces morphismes :*

$$0 \longrightarrow H^0(G,A) \longrightarrow H^0(G,B) \longrightarrow H^0(G,C) \xrightarrow{\nabla} H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \xrightarrow{\nabla} H^2(G,A)\dots$$

*avec $H^0(G,A) = A^G$ et $H^1(G,A)$ l'ensemble que l'on a défini précedemment et qui, dans notre cas, est un groupe abélien parce que A est commutatif.*

**Remarque 2.2.2.** Cet énoncé est encore valable si seul $A$ est supposé commutatif et contenu dans le centre de $B$, on obtient alors une suite exacte de groupes et ensembles pointés :

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

On renvoie à Gille et Szamuely, [6], proposition 4.4.1 pour les détails.

Pour certains groupes $G$, la cohomologie est facile à calculer, notamment pour les groupes cycliques pour lesquels on a des formules très simples pour les $H^n(G,A)$.

**Proposition 2.2.3.** *Soit $G = \langle \sigma \rangle$ un groupe cyclique et soit $A$ un $G$-module. On a alors :*

$$H^n(G,A) = \begin{cases} A^G \text{ si } n = 0 \\ A^G/N_G A \text{ si } n \geq 2 \text{ et } n \text{ pair} \\ A(N_G)/(\sigma - 1)A \end{cases}$$

*avec $N_G = \sum_{g \in G} g$ et $A(N_G) = \{x \in A \mid N_G x = 0\}$.*

De plus, la cohomologie des groupes profinis se ramène à la cohomologie des groupes finis par la formule suivante :

$$H^n(G,A) = \operatorname{colim}_U H^n(G/U, A^U)$$

avec $U$ sous-groupe ouvert distingué de $G$. On montre que les groupes de cohomologie profinie sont toujours des groupes de torsion.

## 2.3 Un premier exemple en théorie de Galois

En cohomologie galoisienne, c'est à dire lorsque $G = G_k$ avec $k$ un corps (parfait), on notera simplement $H^n(k,A)$ pour $H^n(G_k,A)$ et si $\ell/k$ est une extension algébrique, on note aussi $H^n(\ell/k,A)$ pour $H^n(\mathrm{Gal}(\ell/k),A)$. Un des théorèmes fondamentaux de la cohomologie galoisienne est une formulation cohomologique de Hilbert 90.

**Théorème 2.3.1.** *Soit $k$ un corps parfait et $n \geq 1$. L'ensemble de cohomologie suivant est trivial :*

$$H^1(k, \mathrm{GL}_n(\overline{k})) = \{\bullet\}.$$

*De plus, on a aussi $H^m(k,\overline{k}) = 0$ pour tout $m \geq 1$.*

Il est possible de donner une explication assez simple de cet énoncé si l'on est prêt à admettre la philosophie générale des formes tordues : on a $H^1(k,\mathrm{GL}_n(\overline{k})) = H^1(k,\mathrm{Aut}(\overline{k}^n))$ qui classifie les formes tordues du $\overline{k}$-espace vectoriel $\overline{k}^n$, c'est à dire les $k$-espaces vectoriels qui deviennent isomorphes à $\overline{k}^n$ après tensorisation par $\overline{k}$, et on sait bien que les espaces vectoriels sont classifiés par leur dimension, donc il n'y a qu'une seule classe de cohomologie dans ce cas.
Le deuxième énoncé provient du théorème de la base normale (le lecteur trouvera plus de détails dans le livre de Gille et Szamuely [6]).
Voici déjà un premier exemple important d'application de la suite exacte longue en cohomologie galoisienne.

**Exemple 2.3.2.** (Théorie de Kummer)
Soit $k$ un corps parfait et $n$ un entier non-nul dans $k$. On a alors une suite exacte de $G_k$-modules discrets en considérant le morphisme de mise à la puissance $n$, noté $[n]$ :

$$0 \longrightarrow \mu_n \longrightarrow \overline{k}^\times \xrightarrow{[n]} \overline{k}^\times \longrightarrow 0$$

avec $\mu_n$ l'ensemble des racines $n$-èmes de l'unité de $\overline{k}$ (il y en a $n$ car $n \neq 0$ dans $k$). Cette suite exacte induit donc une suite exacte longue qui commence comme ceci :

$$0 \longrightarrow \mu_n(k) \longrightarrow k^\times \xrightarrow{[n]} k^\times \longrightarrow H^1(k,\mu_n) \longrightarrow H^1(k,k^\times)$$

et ce dernier terme est nul par Hilbert 90. On a donc un isomorphisme canonique :

$$k^\times/(k^\times)^n \cong H^1(k, \mu_n)$$

qui envoie la classe de $a \in k^\times$ sur le cocycle $\sigma \mapsto \sigma(b)/b$ avec $b \in \overline{k}$ une racine $n$-ème de $a$.
Supposons maintenant que $k$ possède toutes les racines $n$-èmes de l'unité : $\mu_n \subseteq k$. Dans ce cas, $\mu_n$ est muni d'une action triviale de $G_k$ et il est alors facile de montrer que :

$$H^1(k, \mu_n) \cong \mathrm{Hom}(G_k, \mu_n)$$

où Hom désigne l'ensemble des morphismes de groupes continus. Autrement dit, les caractères du groupe de Galois $G_k$ à valeurs dans $\mu_n$ sont classifiés par le groupe $k^\times/(k^\times)^n$, or un tel caractère correspond (à un automorphisme près) à une extension cyclique de degré divisant $n$ de $k$, en considérant le noyau du caractère puis l'extension fixée par ce noyau. Ceci permet de retrouver la théorie de Kummer, selon laquelle les extensions cycliques de degré divisant $n$ de $k$ s'obtiennent en ajoutant une racine $n$-ème d'un élément de $k^\times$.

## 2.4 Le groupe de Brauer d'un corps parfait

Le deuxième exemple que l'on donne est en lien avec les CSA sur $k$. On avait vu qu'on pouvait classifier les CSA de degré $n$ par l'ensemble $H^1(G_k, \mathrm{PGL}_n(\overline{k}))$ et on va voir à présent comment classifier toutes les CSA sur $k$, non pas à isomorphisme près, mais à *Brauer-équivalence* près. L'avantage est qu'on pourra mettre une structure de groupe sur l'ensemble $\mathrm{Br}(k)$ des classes d'équivalence, appelé groupe de Brauer de $k$, et en donner une description purement cohomologique comme le groupe $H^2(k, \overline{k})$.
Donnons les grandes idées de cette histoire. On commence par définir la Brauer-équivalence.

**Définition 2.4.1.** *Soit $k$ un corps parfait et $A, B$ deux CSA sur $k$. On dit qu'elles sont Brauer-équivalentes s'il existe $p, q \geq 1$ et un isomorphisme de $k$-algèbres :*

$$M_p(A) \cong M_q(B).$$

*On peut montrer qu'une CSA est toujours une algèbre de matrices sur une algèbre à division centrale, et si $A$ est une algèbre de matrices sur $D_A$ et $B$ une algèbre de matrices sur $D_B$ des algèbres à division centrales, alors $A$ et $B$ sont Brauer-équivalentes si et seulement si $D_A \cong D_B$. Ainsi, l'ensemble $\mathrm{Br}(k)$ des classes d'équivalence classifie aussi les algèbres à division sur $k$ à isomorphisme près.*

Notons que deux CSA sont isomorphes si et seulement si elles sont Brauer-équivalentes et de même degré. Le produit tensoriel de deux CSA est encore une CSA, ce qui permet de munir $\mathrm{Br}(K)$ d'une structure de groupe abélien, dont le neutre est donné par la classe de $K$ et l'inverse de la classe d'une CSA $A$ est donné par la classe de l'algèbre opposée $A^{\mathrm{opp}}$.
Ainsi, les exemples du début montrent que :

$$\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$$

par 1.1.1 et

$$\mathrm{Br}(k) = 0$$

pour $k$ un corps fini (c'est le théorème de Wedderburn 1.4.2) ou pour $k$ algébriquement clos ou encore, ce qui englobe ces deux cas, pour $k$ un corps $C_1$ comme on l'a dit plus tôt.

Considérons alors la suite exacte suivante de $G_k$-groupes, le premier étant commutatif et contenu dans le centre du second comme dans la remarque 2.2.2 :

$$0 \longrightarrow \overline{k}^{\times} \longrightarrow \mathrm{GL}_n(\overline{k}) \longrightarrow \mathrm{PGL}_n(\overline{k}) \longrightarrow 0$$

pour $n \geq 1$. On en déduit une suite exacte d'ensembles pointés :

$$\cdots \longrightarrow H^1(k, \mathrm{PGL}_n(\overline{k})) \xrightarrow{\nabla} H^2(k, \overline{k}^{\times}) \longrightarrow \ldots$$

qui permet d'associer à toute CSA de degré $n$ un élément du groupe $H^2(k, \overline{k}^{\times})$. Ceci permet alors de construire un isomorphisme :

$$\mathrm{Br}(k) \cong H^2(k, \overline{k}^{\times})$$

dont le lecteur pourra trouver les détails chez Gille et Szamuely [6]. Avec la suite exacte $0 \longrightarrow \mu_n \longrightarrow \overline{k}^{\times} \xrightarrow{[n]} \overline{k}^{\times} \longrightarrow 0$ et Hilbert 90, on obtient aussi pour $n \neq 0$ dans $k$ :

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

avec $\mathrm{Br}(k)[n]$ la $n$-torsion du groupe de Brauer. Avec cette description et comme $G_{\mathbb{R}}$ est engendré par la conjugaison complexe $\tau$, on retrouve par exemple, par 2.2.3 que :

$$\mathrm{Br}(\mathbb{R}) \cong H^2(\langle\tau\rangle, \mathbb{C}^{\times}) = (\mathbb{C}^{\times})^{\langle\tau\rangle}/(N\mathbb{C}^{\times}) = \mathbb{R}^{\times}/(\mathbb{R}_+^*) \cong \mathbb{Z}/2\mathbb{Z}$$

avec $N(z) = z\overline{z}$.

**Remarque 2.4.2.** Le fait d'avoir une description cohomologique du groupe de Brauer a de nombreux avantages : cela permet de faire rentrer son étude dans une théorie très générale et fonctorielle. On peut par exemple montrer que $H^2(\ell/k, \ell^{\times})$, pour une extension algébrique $\ell/k$, s'identifie aux éléments du groupe de Brauer qui sont des classes d'algèbres qui se déploient sur $\ell$, autrement dit la suite :

$$0 \longrightarrow H^2(\ell/k, \ell^{\times}) \longrightarrow \mathrm{Br}(k) \longrightarrow \mathrm{Br}(\ell)$$

est exacte, ce qui provient de propriétés formelles de la cohomologie (c'est la suite spectrale de Hoschild-Serre) et de Hilbert 90.
Un autre avantage est que la cohomologie possède une structure d'algèbre au sens suivant : si $A$ et $B$ sont deux $G$-modules discrets, on a toujours une opération bilinéaire, appelée le cup-produit :

$$\cup : H^p(G, A) \otimes H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B).$$

Ceci permet par exemple de construire des éléments de $\mathrm{Br}(k) = H^2(k, \overline{k}^{\times})$ à partir d'éléments de $H^1(k, \mu_n)$ par exemple, un groupe plus facile à appréhender. C'est ainsi que l'on construit des algèbres dites cycliques (les algèbres de quaternions en sont un cas particulier pour $n = 2$).
La formulation cohomologique de la théorie du corps de classe local repose fondamentalement sur le calcul du groupe de Brauer du corps $p$-adique $\mathbb{Q}_p$ (voir le livre de Neukirch [5]). En effet, on montre que :

$$\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}.$$

# 3 Propriétés diophantiennes des corps et dimension cohomologique

Comme on a vu précedemment, il est possible de définir une condition de corps $C_1$ qui entraîne que le groupe de Brauer est nul. En fait, on peut montrer beaucoup mieux : pour un corps parfait $k$ qui est $C_1$, on a $H^n(k, A) = 0$ pour tout $G_k$-module discret *de torsion* et pour tout $n \geq 2$. On dit alors que $k$ est de dimension cohomologique au plus 1 (en réalité il y a des subtilités en caractéristique positive que l'on va ignorer). Ceci mérite de donner quelques définitions précises.

**Définition 3.0.1.** *Soit $k$ un corps parfait et $i \geq 0$ un entier. On dit que $k$ est un corps $C_i$ si pour tout $n \geq 1$ et tout polynôme homogène $f$ à coefficients dans $k$ à $n$ variables et de degré $d \geq 1$ avec $d^i < n$, $f$ possède un zéro non-trivial dans $k^n$, non-trivial signifiant différent du vecteur nul.*
*Enfin, on dit que $k$ est de dimension cohomologique au plus $i$ si pour tout $G_k$-module $A$ discret et de torsion et tout $n > i$, on a $H^n(k, A) = 0$.*

En réalité, cette définition de dimension cohomologique est valide en caractéristique nulle mais il faudrait la modifier légèrement pour l'avoir en caractéristique $p$ (on renvoie à l'article de Kato et Kuzumaki qui fonde ces définitions [3]).
Ces deux notions ont de nombreuses similarités bien que leurs définitions soient de natures complétement différentes : la première est une définition purement diophantienne qui fait appel à de la géométrie arithmétique et la seconde ne dépend que du groupe de Galois $G_k$. Voici quelques exemples de similarités entre les deux définitions :

— Un corps parfait $k$ est algébriquement clos si et seulement si sa dimension cohomologique est nulle, et si et seulement s'il est $C_0$.

— Les corps finis sont $C_1$ et de dimension cohomologique 1.

— Si un corps $k$ est $C_i$ et si $\ell/k$ est une extension de degré de transcendance fini $m$, alors $\ell$ est un corps $C_{i+\ell}$ et il en va de même pour la dimension cohomologique. De même, si $k$ est $C_i$, alors le corps $k((T))$ est $C_{i+1}$, et pareil pour la dimension cohomologique.

— Comme on a vu précedemment, la propriété $C_1$ entraîne l'annulation du groupe de Brauer, et on peut montrer que ça entraîne même que la dimension cohomologique est au plus 1. En fait, on conjecture que la propriété $C_i$ en général entraîne que la dimension cohomologique est au plus $i$, et c'est vrai pour $i \in \{0, 1, 2\}$. Une des raisons qui empêche de continuer pour $i \geq 3$ est que l'on ne sait pas associer des polynômes homogènes à des éléments de $K$-théorie de Milnor de degré au moins 3 alors qu'on sait le faire pour les degrés 1 et 2, mais je n'ai pas la place d'en dire plus ici.

Il est alors assez naturel, au vu de toutes ces similarités, de conjecturer que la condition $C_i$ soit équivalente à la condition d'avoir dimension cohomologique au plus $i$. Malheureusement il existe des contre-exemples très simples : le corps $\mathbb{Q}_p$ est de dimension cohomologique 2 mais il n'est pas $C_2$ (on renvoie au livre de Greenberg par exemple [1], chapitre 7).
Kato et Kuzumaki ont alors l'idée d'introduire des conditions plus fines, appelées $C_i^q$ qui sont construites à partir de la $K$-théorie de Milnor du corps $k$, pour lesquelles on a vraiment :

$$C_0^q \iff \text{dimension cohomologique au plus } q$$

et conjecturalement $C_i^q \iff C_p^j$ dès que $q + i = j + p$. Malheureusement cette deuxième conjecture, dite de Kato et Kuzumaki et présentée dans l'article *The dimension of fields and algebraic K-theory* [3]

est encore fausse mais cette fois-ci les contre-exemples sont très délicats à construire (voir [4]), et il est naturel de se demander si elle peut rester vraie pour les corps de la vie de tous les jours.

Voici un rapide état de l'art quant à ces conjectures :

— Kato et Kuzumaki montrent une forme plus faible de la conjecture en restreignant les polynômes à être de degré 2 et d'une certaine forme (ce sont des formes de Pfister), puis de degré premier pour certaines propriétés de transition du corps résiduel $k$ d'un anneau de valuation discrète complet $R$ au corps des fractions $K$.

— Olivier Wittenberg démontre dans son article [10] que les corps $p$-adiques et les corps de nombres totalement imaginaires sont $C_1^1$ par des arguments de dévissage et de résolution des singularités en se ramenant à de la géométrie sur des variétés régulières. Il démontre aussi des propriétés de transition de propriétés $C_1^q$ plus faibles pour le passage du corps résiduel $k$ d'un anneau de valuation discrète complet $R$ au corps des fractions $K$.

— Diego Izquierdo, mon encadrant de stage de M2, traite le cas des corps de fonctions sur un corps algébriquement clos, et donne une preuve différente de celle de Wittenberg, plus explicite et basée sur un passage local global, du fait que les corps de nombres totalement imaginaires sont $C_1^1$. Il traite aussi le cas des corps $K((t))$ avec K un corps de fonctions d'une variété intègre sur un corps algébriquement clos. Dans un second article avec Giancarlo Lucchini Arteche, il démontre aussi la propriété $C_2^2$ pour les corps de fonctions de courbes $p$-adiques, et un résultat partiel en direction de la condition $C_1^2$ qui serait attendue par la conjecture de Kato et Kuzumaki.

# 4 Pour aller plus loin

Donnons enfin quelques pistes d'ouverture dans ce domaine.

Pour définir proprement les conditions $C_i^q$ évoquées plus haut, il faut construire la $K$-théorie de Milnor d'un corps $k$, qui est une construction complétement explicite de groupes $K_n(k)$ qui forment ensemble un anneau gradué. Plus précisément, on pose :

$$K_*(k) = \bigoplus_{n\geq 0} K_n(k)$$

défini comme le quotient de l'algèbre tensorielle $T_{\mathbb{Z}}(k^\times)$ du groupe abélien $k^\times$ par l'idéal gradué engendré par les $x\otimes(1-x)$ pour $x, 1-x \in k^\times$. En particulier on a donc $K_0(k) = \mathbb{Z}$ puis $K_1(k) = k^\times$.
Si $a_1,\dots,a_n \in k^\times$, on note généralement $\{a_1,\dots,a_n\}$ la classe de $a_1\otimes\cdots\otimes a_n$ dans $K_n(k)$ et si $u, v \in K_*(k)$ on note aussi $\{u,v\}$ ou bien $uv$ leur produit dans $K_*(k)$. La structure additive de l'anneau $K_*(k)$ sera notée + bien qu'elle provienne de la structure multiplicative de $k$.
Grâce au cup-produit en cohomologie, on a alors, pour tout $m$ premier avec la caractéristique de $k$ et tout $n \geq 0$, un morphisme :

$$(k^\times)^{\otimes n} \longrightarrow H^n(k, \mu_m)$$

obtenu à partir du morphisme $k^\times \longrightarrow H^1(k,\mu_m)$ qui vient de la suite exacte $0 \longrightarrow \mu_m \longrightarrow \overline{k}^\times \longrightarrow \overline{k}^\times \longrightarrow 0$. On peut montrer (c'est fait dans le livre de Gille et Szamuely [6] par exemple) que ce morphisme se factorise par la $K$-théorie de Milnor et donne un morphisme d'anneaux :

$$h_* : K_*(k)/mK_*(k) \longrightarrow \bigoplus_{n\geq 0} H^n(G, \mu_m^{\otimes n}).$$

**Théorème 4.0.1.** *La conjecture de Bloch-Kato, démontrée par Voevodsky et Rost (voir [8]) et ainsi devenue le théorème d'isomosphisme de norme et résidu, affirme alors que :*

$$h_* : K_*(k)/(m) \longrightarrow \bigoplus_{n\geq 0} H^n(G, \mu_m^{\otimes n})$$

*est un isomorphisme d'anneaux gradués.*

Ce théorème permet d'appréhender la cohomologie à valeurs dans $\mu_m$ de façon combinatoire. Pour $n = 2$, on obtient que le groupe de Brauer est engendré par les algèbres cycliques et pour $m = 2$ on peut faire le lien avec la théorie des formes quadratiques sur $k$.

Dans une autre direction, il est possible de généraliser la cohomologie galoisienne pour y apporter une saveur plus géométrique. On obtient ainsi la cohomologie étale sur un schéma $X$, et la cohomologie galoisienne est alors le cas particulier de la cohomologie étale lorsque le schéma $X$ est un point de la forme Spec $k$ avec $k$ un corps. Cela s'inscrit dans la théorie très générale de la cohomologie des faisceaux sur un site, dont on peut trouver une très bonne introduction dans le livre de Tamme [9] intitulé *Introduction to Étale Cohomology*. Ces théories cohomologiques ont des applications dans la théorie des points rationnels et je termine cette note en renvoyant au livre de Poonen [7] pour une introduction à ces idées.

# Références


[1] Marvin J. Greenberg. *Lectures on Forms in Many Variables*. 1968.

[2] Diego Izquierdo. On a conjecture of kato and kuzumaki, 2017. URL : https://perso.pages.math.cnrs.fr/users/diego.izquierdo/media/Research/Kato_Kuzumaki_revision_19_10_2017.pdf.

[3] Takako Kuzumaki Kazuya Kato. The dimension of fields and algebraic k-theory. *Journal of Number Theory*, 24(2) :229–244, 1986. URL : https://www.sciencedirect.com/science/article/pii/0022314X86901058, doi:10.1016/0022-314X(86)90105-8.

[4] Alexander S. Merkurjev. Simple algebras and quadratic forms. *Séminaire Bourbaki*, 1991.

[5] Jürgen Neukirch. *Class Field Theory*. Springer, 1986.

[6] Tamás Szamuely Philippe Gille. *Central Simple Algebras and Galois Cohomology*. Cambridge, 2012.

[7] Bjorn Poonen. *Rational Points on Varieties*. 2010.

[8] Joël Riou. La conjecture de bloch-kato [d'après m. rost et v. voevodsky]. *Séminaire Bourbaki*, 2012.

[9] Günter Tamme. *Introduction to Étale Cohomology*. Springer, 1994.

[10] Olivier Wittenberg. Sur une conjecture de kato et kuzumaki concernant les hypersurfaces de fano. *Duke Mathematical Journal*, 2015. URL : http://dx.doi.org/10.1215/00127094-3129488.