Introduction à la conjecture de Kato et Kuzumaki

Louis Mallet-Burgues

Sous la direction de Diego Izquierdo

30 Août 2025

Table des matières

Introduction

Le but de ce mémoire est de présenter tout ce que j'ai appris sur la conjecture de Kato et Kuzumaki en géométrie arithmétique pendant mon stage de master 2 sous la direction de D. Izquierdo, stage qui s'est officiellement déroulé à polytechnique et officieusement dans les bureaux de Jussieu et dans la bibliothèque de l'ENS. On y donne aussi une idée générale des outils de cohomologie et de géométrie algébrique qui interviennent dans la formulation de cette conjecture et dans les preuves de ses résultats partiels. Cela en fait un document assez long, mais la plupart des chapitres peuvent-être vus comme des prérequis pour les chapitres 6, 7, 8 et 9 qui sont le cœur du sujet. J'ai fait en sorte que ce texte soit le plus complet possible pour un étudiant qui voudrait comprendre le sujet avec les mêmes connaissances que moi quand j'ai commencé ce stage.

La conjecture qui nous intéresse propose de relier des invariants de natures assez différentes que l'on peut associer à un corps K. Le premier invariant, la *dimension cohomologique*, est plutôt abstrait, et ne porte que sur le groupe de Galois absolu $G_K = \mathrm{Gal}(K_s/K)$ avec K_s une clôture séparable de K. De façon informelle et imprécise (surtout en caractéristique positive), la dimension cohomologique de K est le plus grand entier au delà duquel le groupe profini G_K n'a plus de cohomologie à valeur dans des modules topologiques de torsion. Historiquement, la première tentative de relier cet invariant à quelque chose de plus concret est d'introduire la propriété C_i de Lang. Celle-ci est une condition purement *diophantienne* qui porte sur l'existence de zéros non-triviaux à des équations homogènes à beaucoup de variables et petit degré sur le corps K. Plus précisément, on dira que K est un corps C_i si pour tout $n \geq 1$ et pour tout polynôme homogène f à n variables de degré $d \geq 1$ avec $d^i < n$, f possède un zéro non-trivial dans K (car 0 est toujours un zéro de f).

Ces deux invariants ont beaucoup de similarités. Par exemple, seuls les corps algébriquement clos sont C_0 et de dimension cohomologique nulle, et les corps finis sont de dimension cohomologique 1 et sont C_1 par un théorème de Chevalley-Warning. De plus, lorsque l'on passe à une extension algébrique, le caractère C_i et la dimension cohomologique restent tous deux inchangés. La propriété C_i se comporte bien aussi vis à vis des extensions transcendantes : si K est C_i, alors $K(T)$ est C_{i+1}, et on a le même comportement pour $K((T))$. Chacun des deux invariants a ses avantages et il est naturel de se demander s'ils sont reliés : est-ce qu'un corps vérifie la propriété C_i si et seulement si sa dimension cohomologique est au plus i ? Il se trouve que la réponse est négative avec un contre-exemple assez simple : le corps $\mathbb{Q}_p$ est de dimension cohomologique 2 mais n'est pas un corps C_2. Il faut donc raffiner la notion de corps C_i pour espérer obtenir un vrai résultat.

Une première idée est de remplacer la condition de l'existence de zéros non-triviaux (autrement dit de points rationnels de $X = V(f)$ l'hypersurface définie par f) par la condition plus arithmétique d'existence de 0-cycles de degré 1 sur X, autrement dit de points fermés x_i de X définis sur des corps K_i de degrés sur K premiers entre eux. On obtient alors (à un détail près) une condition dite C_i^0 qui est un peu plus satisfaisante. Kato et Kuzumaki introduisent alors toute une famille de propriétés commençant par C_i^0 et terminant par C_0^i (cette dernière étant équivalente à dire que K est de dimension cohomologique au plus i), avec entre les deux les C_j^q avec $i = j + q$ et espèrent que toutes ces

propriétés soient deux à deux équivalentes.

Pour définir la condition C_i^q, on a besoin de construire la K-théorie de Milnor du corps K, que l'on peut voir comme un anneau gradué $K_*(K) = \bigoplus_{q\geq 0} K_q(K)$ commutatif au sens gradué, avec notamment $K_0(K) = \mathbb{Z}$ et $K_1(K) = K^\times$. C'est un invariant assez facile à définir qui a l'avantage d'être suffisament fonctoriel pour ressembler à de la cohomologie : si L/K est une extension finie, on a des morphismes de norme :

$$K_q(L) \xrightarrow{N_{L/K}} K_q(K)$$

qui ont de bonnes propriétés et qui donnent en degré 1 la norme usuelle et en dégré 0 la multiplication par $[L : K]$. On définit alors la propriété C_i^q de la façon suivante : K est C_i^q si pour toute extension finie L/K et tout polynôme homogène f à coefficients dans L de degré d à $n > d^i$ variables, le groupe $K_q(L)$ est engendré par les images des morphismes de normes $N_{L(x)/L} : K_q(L(x)) \longrightarrow K_q(L)$ avec x point fermé de l'hypersurface définie par x.
La conjecture de Bloch-Kato démontrée plus tard par Voevodsky et Rost donne alors un lien important entre la cohomologie galoisienne et la K-théorie de Milnor en stipulant que l'on a un isomorphisme canonique :

$$H^n(K, \mu_m^{\otimes n}) \cong K_n(K)/mK_n(K)$$

pour tout n et pour tout m. Ceci permet de voir que la condition C_0^q équivaut à ce que K ait dimension cohomologique au plus q.

On peut alors énoncer la conjecture de Kato et Kuzumaki.

Conjecture 0.0.0.1. *(Kato, Kuzumaki)*
Soit K un corps et i, q des entiers naturels. Les conditions suivantes sont équivalentes :

- *La dimension cohomologique de K est au plus $i + q$.*
- *Le corps K vérifie la condition C_i^q.*

Encore une fois, cette conjecture est fausse mais les contre-exemples sont délicats à construire : Merkurjev construit un corps de caractéristique nulle qui est de dimension cohomologique 2 mais pas C_2^0 dans [17], en utilisant une méthode de récurrence transfinie. C'est donc assez naturel de se demander si la conjecture est vraie pour des corps de la vie de tous les jours comme des corps de fonctions, des corps de nombres et des corps construits à partir de ceux-ci.

Les trois articles qui donnent le fil directeur de ce mémoire sont les suivants.

- L'article fondateur de Kato et Kuzumaki [14], où ils traitent entièrement le cas de la conjecture restreinte à certains polynômes de degré 2, appelés formes de Pfister, et où ils étudient des propriétés de transitivité de la condition C_i^q pour les corps à valuation discrète.
- L'article de Wittenberg [30] qui introduit la condition C_1^q forte et démontre que les corps p-adiques et les corps de nombres totalement imaginaires sont C_1^1 via des arguments de dévissage et de résolution des singularités.
- L'article d'Izquierdo [10] qui traite le cas des corps de fonctions sur un corps algébriquement clos, et qui donne une preuve différente de celle de Wittenberg, plus explicite et basée sur un passage local global pour un certain tore multinormique, du fait que les corps de nombres totalement imaginaires (resp. les corps globaux de caractéristique positive) sont C_1^1 (resp. vérifient une condition du type C_1^1 *en dehors de la caractéristique*). Il traite aussi le cas des corps $K((t))$ avec K un corps de fonctions d'une variété intègre sur un corps algébriquement clos.

Le mémoire commence par une invitation au langage des faisceaux sur un site et à leur cohomologie (chapitre 1), une façon d'incorporer toutes les théories cohomologiques qui interviendront dans la suite. On met l'accent sur l'interprétation du H^1 comme un ensemble de torseurs, une idée omniprésente en géométrie arithmétique, et on traite le cas particulier de la cohomologie des groupes (profinis).

Le chapitre 2 décrit le cas particulier de la cohomologie galoisienne d'un corps K, qui s'interpréte à la fois comme la cohomologie du groupe de Galois absolu G_K et comme la cohomologie étale sur $\mathrm{Spec}(K)$. On y présente aussi la notion d'algèbre centrale simple ainsi que le groupe de Brauer de K qui les classifie. On parle ensuite de dimension cohomologique des corps et on termine par quelques propriétés sur les groupes de Tate-Chaffarevich qui mesurent le défaut de passage local-global de la cohomologie pour les corps globaux.

Au chapitre 3, on fait quelques rappels sur les groupes algébriques sur un corps et on utilise la dualité de Poitou-Tate pour obtenir l'annulation du premier groupe de Tate-Chaffarevich de certains tores définis par des équations de norme, un résultat de Demarche et Wei publié dans [2]. On généralise ce résultat à des tores "de dimension infinie" pour pouvoir l'appliquer plus tard à la conjecture de Kato et Kuzumaki pour les corps de nombres totalement imaginaires.

Au chapitre 4, on introduit le deuxième ingrédient phare des conjectures de Kato et Kuzumaki : la K-théorie de Milnor d'un corps et ses propriétés fonctorielles. On se base sur le livre de Gille et Szamuely [20] et on explique le lien avec la théorie des formes quadratiques via la conjecture de Milnor (prouvée par Voevodsky, Orlov et Vishik), ainsi que le lien avec la cohomologie galoisienne via la conjecture de Bloch-Kato (prouvée par Voevodsky et Rost).

Le chapitre 5 se base sur l'article de Borel et Serre [1] et sur le livre [3] de Harris et Eisenbud pour donner quelques éléments de théorie de l'intersection et classes de Chern sur les schémas. On y présente un théorème de dévissage de Wittenberg 5.2.0.2 qui sera crucial dans la suite pour ramener l'étude de propriétés arithmétiques de certains schémas à des schémas plus simples et plus réguliers.

Le chapitre 6 introduit les propriétés C_i et C_i^q des corps et leurs premières propriétés en se basant sur l'article de Kato et Kuzumaki [14] ainsi que sur le livre de Greenberg [5].

Les chapitres 7 et 8 sont basés sur l'article de Wittenberg [30] et ont pour but d'établir des propriétés diophantiennes des corps p-adiques, et le chapitre 9 présente les preuves de Wittenberg et Izquierdo du fait que les corps de nombres totalement imaginaires vérifient la propriété C_1^1.

Je tiens à remercier chaleureusement mon encadrant Diego Izquierdo qui a su me guider à travers un sujet passionant et très nouveau pour moi et qui a toujours été de bon conseil même quand nous étions de part et d'autre de l'Atlantique. Je remercie aussi Gaëtan Chenevier pour m'avoir mis en contact avec Diego et je salue mes amis et voisins de table à la bibliothèque de l'ENS avec qui ça a toujours été un plaisir de partager les pauses café et les repas du midi. Ce stage m'a permis d'apprendre une quantité d'outils pour appréhender la géométrie arithmétique depuis le peu que j'en connaissais et j'aurais voulu, si le temps l'avait permis, en apprendre davantage pour démystifier les boîtes noires qui figurent dans ce mémoire. Je termine donc cette introduction en recommandant le livre de Poonen [22] qui donne une introduction passionante avec le juste niveau de détail au domaine des points rationnels sur les variétés.

Chapitre 1

Un horizon des théories cohomologiques

1.1 Cohomologie des faisceaux sur un site

Le but de cette partie est de rapidement présenter sans faire de preuves le cadre unificateur dans lequel Grothendieck définit la cohomologie des faisceaux. On pourra trouver plus de détails dans [28]. Pour simplifier, le choix est fait ici d'ignorer les aspects problématiques de théorie des ensembles dûs à la taille des objets que l'on considère : dans les applications, la collection des recouvrements d'un objet dans une topologie de Grothendieck pourra être identifiée à un ensemble.

1.1.1 Topologies de Grothendieck et faisceaux

L'idée de départ de Grothendieck est de généraliser la notion d'espace topologique qui servent simplement comme lieu de définition des faisceaux. Pour cela, il introduit la notion de site, c'est à dire de catégorie $\mathcal{C}$ munie d'une topologie $\mathcal{T}$. Les faisceaux sur le site $(\mathcal{C},\mathcal{T})$, ou pour simplifier, sur le site $\mathcal{C}$, seront alors des cas particuliers de préfaisceaux sur la catégorie $\mathcal{C}$, c'est à dire des foncteurs de $\mathcal{C}^{\mathrm{opp}}$ vers Set, ou vers Ab ou tout autre catégorie raisonnable.

Définition 1.1.1.1. *(Site de Grothendieck)*
Soit $\mathcal{C}$ une catégorie. Une topologie sur $\mathcal{C}$ consiste en la donnée, pour chaque objet U de $\mathcal{C}$, d'une famille de recouvrements, c'est à dire de familles de morphismes $(U_i \longrightarrow U)_i$ avec les propriétés suivantes :

- *Les recouvrements sont préservés par tirés en arrière, au sens où pour chaque recouvrement $(U_i \longrightarrow U)_i$ et pour chaque $f : V \longrightarrow U$, les produits fibrés $U_i \times_U V$ existent et $(U_i \times_U V \longrightarrow V)_i$ est un recouvrement de V.*
- *Si $(U_i \longrightarrow U)_i$ est un recouvrement de U et que pour tout i, $(V_{ij} \longrightarrow U_i)_j$ est un recouvrement de U_i, alors $(V_{ij} \longrightarrow U)_{i,j}$ est un recouvrement de U.*
- *Si $U' \longrightarrow U$ est un isomophisme, alors la famille a un seul élément $(U' \longrightarrow U)$ est un recouvrement de U.*

Lorsque $\mathcal{C}$ est munie d'une topologie $\mathcal{T}$, on dit que c'est un site.
Un morphisme de sites $f : \mathcal{C} \longrightarrow \mathcal{C}'$ est un foncteur qui envoie les recouvrements sur des recouvrements et qui vérifie de plus que pour tout recouvrement $(U_i \longrightarrow U)$ de $\mathcal{C}$ et tout $V \longrightarrow U$ dans $\mathcal{C}$, le morphisme canonique :

$$f(U_i \times_U V) \longrightarrow f(U_i) \times_{f(U)} f(V)$$

est un isomorphisme, c'est à dire que f préserve certains produits fibrés.

Il est possible de définit la notion de faisceaux sur un site. On rappelle qu'un préfaisceau d'ensembles (resp. de groupes abéliens) sur une catégorie $\mathcal{C}$ est un foncteur de $\mathcal{C}^{\mathrm{opp}}$ vers Set (resp. Ab).

Définition 1.1.1.2. *(Faisceaux sur un site)*
Un faisceau d'ensembles $\mathcal{F}$ (resp. de groupes abéliens) sur un site $\mathcal{C}$ est un préfaisceau sur $\mathcal{C}$ à valeurs dans Set *(resp. dans* Ab*), qui vérifie la condition de recollement suivante : pour tout recouvrement $(U_i \longrightarrow U)$, en notant $U_{ij} = U_i \times_U U_j$, le morphisme canonique $\mathcal{F}(U) \longrightarrow \prod_i \mathcal{F}(U_i)$ induit un isomorphisme entre $\mathcal{F}(U)$ et la limite du diagramme suivant :*

$$\prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_{ij})$$

Cette définition a l'avantage de généraliser des quantités d'exemples.

Exemple 1.1.1.3. — Si X est un espace topologique, on lui associe le site formée par la catégorie des ouverts de X ordonnés par l'inclusion, où les recouvrements sont les $(U_i \longrightarrow U)$ tels que $\bigcup_i U_i = U$. On retrouve alors la notion usuelle de faisceaux sur un espace topologique. On notera que si $f : X \longrightarrow Y$, est une application continue, on obtient un morphisme de sites $Y \longrightarrow X$: on retiendra que les morphismes de sites vont dans le sens *anti-géométrique*.

— Si $\mathcal{C}$ est une catégorie quelconque, la topologie *discrète* est celle où les seuls recouvrements sont les familles composés d'un seul isomorphisme. Pour cette topologie, la notion de préfaisceau coïncide avec la notion de faisceau.

— Si $\mathcal{C}$ est une catégorie quelconque avec produits fibrés, la topologie *canonique* sur $\mathcal{C}$ est la topologie la plus fine (i.e. avec le plus de recouvrements) telle que les préfaisceaux représentables soient des faisceaux. Concrètement, on dit qu'une famille $(U_i \longrightarrow U)$ est *pré-couvrante* si pour tout objet Z, on a un isomorphisme canonique entre $\mathrm{Hom}(V, Z)$ et la limite du diagramme suivant :

$$\prod_i \mathrm{Hom}(U_i, Z) \rightrightarrows \prod_{i,j} \mathrm{Hom}(U_{i,j}, Z)$$

et on dit qu'elle est couvrante si pour tout $V \longrightarrow U$, la famille obtenue par tiré en arrière sur V est pré-couvrante. On peut alors vérifier que les familles couvrantes forment une topologie sur $\mathcal{C}$, qui est bien la plus fine faisant des préfaisceaux représentables des faisceaux.

— Si G est un groupe, on munit la catégorie des G-ensembles à gauche, $G-\mathrm{Set}$, de la topologie canonique. Comme on le verra dans la partie sur la cohomologie des groupes, les faisceaux d'ensembles sur ce site s'identifient aux G-ensembles (à gauche) et les faisceaux de groupes abéliens s'identifient aux G-modules (à gauche). On verra aussi qu'il existe une version de ceci pour les groupes profinis.

— La catégorie des sites de Grothendieck possède un objet final qui correspond au site associé à l'espace topologique à un point, ou encore à la catégorie à un seul objet et une seule flèche avec la topologie discrète. Les (pré)faisceaux d'ensembles (resp. de groupes abéliens) sur ce site s'identifient aux ensembles et aux groupes abéliens.

— Si X est un schéma, on munit la catégorie des schémas étales au dessus de X, notée X_{et}, de la topologie de Grothendieck dont les recouvrements sont les familles $U_i \longrightarrow X$ de morphismes étales au dessus de X dont les images recouvrent X topologiquement. On parle alors du *site étale* de X.

1.1.2 Préfaisceaux et faisceaux abéliens sur un site

Si $\mathcal{C}$ est un site, on note $\mathrm{Sh}(\mathcal{C})$ la catégorie des faisceaux de groupes abéliens sur $\mathcal{C}$ et $\mathrm{PSh}(\mathcal{C})$ la catégorie des préfaisceaux de groupes abéliens sur $\mathcal{C}$. Beaucoup des résultats qui suivent s'adaptent d'ailleurs aux faisceaux et préfaisceaux d'ensembles.
Comme pour les espaces topologiques, il est possible de *faisceautiser* un préfaisceau sur un site $\mathcal{C}$ (sous des hypothèses raisonnables de nature ensembliste sur la catégorie $\mathcal{C}$). Pour cela, on commence par définir la *cohomologie à la Čech* des préfaisceaux sur un site.
La catégorie $\mathrm{PSh}(\mathcal{C})$ est une catégorie abélienne avec assez d'injectifs, et l'exactitude d'une suite de préfaisceaux $\mathcal{P}_1 \longrightarrow \mathcal{P}_2 \longrightarrow \mathcal{P}_3$ équivaut à l'exactitude pour chaque objet U de la suite de groupes abéliens $\mathcal{P}_1(U) \longrightarrow \mathcal{P}_2(U) \longrightarrow \mathcal{P}_3(U)$. On peut donc dériver des foncteurs additifs définis sur cette catégorie.

Définition 1.1.2.1. *(Cohomologie à la Čech)*
Soit $\mathcal{P}$ un préfaisceau de groupes abéliens sur un site $\mathcal{C}$. On définit, pour tout recouvrement $(U_i \longrightarrow U)_i$, le groupe $\check{H}^0((U_i), \mathcal{P})$ comme la limite du diagramme :

$$\prod_i P(U_i) \rightrightarrows \prod_{i,j} P(U_{ij})$$

Ceci définit un foncteur exact à gauche $\check{H}^0((U_i), \bullet) : \mathrm{PSh}(\mathcal{C}) \longrightarrow \mathrm{Ab}$ que l'on dérive à droite pour obtenir des foncteurs $\check{H}^n((U_i), \mathcal{P})$ de cohomologie à la Čech.

L'avantage de ces groupes de cohomologie à la Čech est qu'ils peuvent se calculer de façon combinatoire, comme la cohomologie du complexe $C^\bullet((U_i), \mathcal{P})$ défini par :

$$C^n((U_i), \mathcal{P}) = \prod_{i_0, \ldots, i_n} \mathcal{P}(U_{i_0, \ldots, i_n})$$

avec encore la notation $U_{i_0,\ldots,i_n} = U_{i_0} \times_U \cdots \times_U U_{i_n}$. On renvoie à [28], Chapitre 1, théorème 2.2.3 pour les détails.
En faisant varier le recouvrement (U_i) de U, il est possible de définir des groupes de cohomologie à la Čech de $\mathcal{P}$ sur U qui ne dépendent pas d'un recouvrement. Pour cela, on définit un raffinement de recouvrements de U, $(U'_j)_{j \in J} \longrightarrow (U_i)_{i \in I}$ comme une application $\varepsilon : J \longrightarrow I$ et une famille de morphismes au dessus de U, $U'_j \longrightarrow U_{\varepsilon(j)}$. On obtient alors une catégorie des recouvrements de U, et on pose :

$$\check{H}^n(U, \mathcal{P}) = \operatorname{colim} \check{H}^n((U_i), \mathcal{P})$$

avec la colimite qui porte sur la catégorie des recouvrements de U.
Il se trouve que le morphisme $\check{H}^n((U'_i), \mathcal{P}) \longrightarrow \check{H}^n((U_i), \mathcal{P})$ est indépendant du choix d'un raffinement (s'il en existe un) et donc on peut aussi voir $\check{H}^n(U, \mathcal{P})$ comme la colimite *filtrante* des $\check{H}^n((U_i), \mathcal{P})$ indexée par la collection ordonnée des recouvrements de U. Le foncteur $\check{H}^0(U, \bullet)$ est alors additif et exact à gauche et ses foncteurs dérivés s'identifient naturellement aux $\check{H}^n(U, \bullet)$. Notons qu'en faisant varier U, on obtient des préfaisceaux $\check{H}^n(\bullet, \mathcal{P})$ associés à $\mathcal{P}$. On pose d'ailleurs :

$$\mathcal{P}^+ = \check{H}^0(\bullet, \mathcal{P}).$$

Avant de définir le processus de faisceautisation, on introduit la notion de préfaisceau séparé.

Définition 1.1.2.2. *(Préfaisceau séparé)*
Un préfaisceau $\mathcal{P}$ sur un site $\mathcal{C}$ est dit séparé si pour tout recouvrement $(U_i \longrightarrow U)$, $\mathcal{P}(U)$ s'injecte dans la limite du diagramme :

$$\prod_i P(U_i) \rightrightarrows \prod_{i,j} P(U_{ij})$$

De façon équivalente, $\mathcal{P}$ est séparé si le morphisme canonique $\mathcal{P} \longrightarrow \mathcal{P}^+$ est injectif.

On montre alors que $\mathcal{P}^+$ est toujours séparé, et que si $\mathcal{Q}$ est un préfaisceau séparé, alors $\mathcal{Q}^+$ est toujours un faisceau. Ceci motive la définition suivante.

Définition 1.1.2.3. *(Faisceautisation)*
Soit $\mathcal{P}$ un préfaisceau sur un site $\mathcal{C}$. On définit son faisceautisé par $\mathcal{P}^s = \mathcal{P}^{++}$. On dispose alors d'un morphisme $\mathcal{P} \longrightarrow \mathcal{P}^s$ qui est l'unité d'une adjonction :

$$\mathrm{Hom}(\mathcal{P}, \mathcal{F}) \cong \mathrm{Hom}(\mathcal{P}^s, \mathcal{F})$$

pour tout préfaisceau $\mathcal{P}$ et tout faisceau $\mathcal{F}$ sur $\mathcal{C}$.

La catégorie $\mathrm{Sh}(\mathcal{C})$ est abélienne, cependant on fera attention au fait que l'inclusion $\mathrm{Sh}(\mathcal{C}) \longrightarrow \mathrm{PSh}(\mathcal{C})$ est seulement exacte à gauche : ce n'est donc pas une sous-catégorie abélienne. Le conoyau d'un morphisme de faisceau est en fait le faisceautisé du conoyau dans la catégorie $\mathrm{PSh}(\mathcal{C})$. Le foncteur de faisceautisation est, quant à lui, exact. Enfin, la catégorie $\mathrm{Sh}(\mathcal{C})$ possède, elle aussi, suffisament d'injectifs.
On peut donc définir la cohomologie des faisceaux en dérivant le foncteur des sections.

Définition 1.1.2.4. *(Cohomologie des faisceaux sur un site)*
Soit $\mathcal{C}$ un site. Pour tout U objet de $\mathcal{C}$, le foncteur $\mathrm{Sh}(\mathcal{C}) \longrightarrow \mathrm{Ab}$ des sections sur U est exact à gauche et donc on peut définir les foncteurs $H^n(U, \bullet) : \mathrm{Sh}(\mathcal{C}) \longrightarrow \mathrm{Ab}$ en dérivant à droite le foncteur des sections sur U. Ceci définit en particulier les groupes de cohomologie des faisceaux $H^n(U, \mathcal{F})$ associés à un faisceau $\mathcal{F}$ sur le site $\mathcal{C}$. Ces groupes sont également fonctoriels en U : si $V \longrightarrow U$ est un morphisme dans $\mathcal{C}$, on obtient un morphisme canonique $H^n(U, \mathcal{F}) \longrightarrow H^n(V, \mathcal{F})$ de restriction qui provient du morphisme de foncteurs $H^0(U, \bullet) \longrightarrow H^0(V, \bullet)$.

Il est alors possible de relier la cohomologie des faisceaux à la cohomologie à la Čech. Pour cela, notons $i : \mathrm{Sh}(\mathcal{C}) \longrightarrow \mathrm{PSh}(\mathcal{C})$ l'inclusion des faisceaux dans les préfaisceaux. Ce foncteur étant exact à gauche et la catégorie des faisceaux ayant assez d'injectifs, on dispose des foncteurs dérivés à droite de i, que l'on note $\mathcal{H}^n : \mathrm{Sh}(\mathcal{C}) \longrightarrow \mathrm{PSh}(\mathcal{C})$. On montre alors que ces foncteurs vérifient :

$$\mathcal{H}^n(\mathcal{F})(U) = H^n(U, \mathcal{F})$$

pour tout objet U de $\mathcal{C}$ et tout faisceau $\mathcal{F}$. La composée de foncteurs :

$$\Gamma_U = \left(\mathrm{Sh}(\mathcal{C}) \xrightarrow{i} \mathrm{PSh}(\mathcal{C}) \xrightarrow{\check{H}^0(U, \bullet)} \mathrm{Ab} \right)$$

avec Γ_U le foncteur des sections sur U induit, par le théorème de Grothendieck et parce que l'image par i de tout injectif est encore injectif donc Γ_U-acyclique, une suite spectrale :

$$\check{H}^q(U, \mathcal{H}^p(\mathcal{F})) \implies H^{p+q}(U, \mathcal{F}).$$

De même, pour tout recouvrement $(U_i \longrightarrow U)$, en considérant la composée :

$$\Gamma_U = \left(\mathrm{Sh}(\mathcal{C}) \xrightarrow{i} \mathrm{PSh}(\mathcal{C}) \xrightarrow{\check{H}^0((U_i),\bullet)} \mathrm{Ab} \right)$$

on a une suite spectrale :

$$\check{H}^q((U_i), \mathcal{H}^p(\mathcal{F})) \implies H^{p+q}(U, \mathcal{F}).$$

En analysant les premiers termes de cette suite spectrale, on construit des morphismes fonctoriels :

$$\check{H}^n((U_i), \mathcal{F}) \longrightarrow H^n(U, \mathcal{F})$$

et :

$$\check{H}^n(U, \mathcal{F}) \longrightarrow H^n(U, \mathcal{F}).$$

Pour $n = 0, 1$, on obtient aussi que le morphisme $\check{H}^n(U, \mathcal{F}) \longrightarrow H^n(U, \mathcal{F})$ est un isomorphisme, et pour $n = 2$ qu'il est injectif.

1.1.3 Poussé en avant et tiré en arrière au niveau des préfaisceaux

Considérons $f : \mathcal{C} \longrightarrow \mathcal{C}'$ un foncteur entre catégories. Pour tout préfaisceau $\mathcal{P}'$ sur $\mathcal{C}'$, on définit le préfaisceau *poussé en avant* :

$$f_{(*)}\mathcal{P}'(U) = \mathcal{P}'(f(U))$$

comme préfaisceau sur $\mathcal{C}$.

Remarque 1.1.3.1. Pour des raisons géométriques (voir l'exemple 1.1.1.3), on choisit d'appeler poussé en avant ce qui semble être un tiré en arrière au niveau des catégories (ou plus loin, au niveau des sites) : cela vient du fait que dans nos exemples, les sites seront associés à des espaces géométriques et les morphismes de sites proviendront de morphismes entre ces espaces géométriques dans *l'autre sens*. Dans le livre de Tamme [28], ce que l'on note $f_{(*)}$ est noté f^p. Ce sera aussi le cas pour le foncteur $f^{(*)}$ ainsi que pour les foncteurs f_* et f^* au niveau des faisceaux.

Le tiré en arrière est alors construit de façon à être un adjoint à gauche du poussé en avant.

Proposition 1.1.3.2. *Soit $f : \mathcal{C} \longrightarrow \mathcal{C}'$ un foncteur entre catégories. Le foncteur de poussé en avant $f_{(*)} : \mathrm{PSh}(\mathcal{C}') \longrightarrow \mathrm{PSh}(\mathcal{C})$ possède un adjoint à gauche, noté $f^{(*)} : \mathrm{PSh}(\mathcal{C}) \longrightarrow \mathrm{PSh}(\mathcal{C}')$, appelé tiré en arrière.*
Le foncteur $f_{(*)}$ est exact et son adjoint à gauche $f^{(*)}$ est exact à droite. Si de plus $f^{(*)}$ est exact, alors $f_{(*)}$ envoie les injectifs sur des injectifs.

Démonstration. Détaillons la construction de cet adjoint à gauche. Soit $\mathcal{P}$ un préfaisceau sur $\mathcal{C}$ et U' un objet de $\mathcal{C}'$. On pose :

$$f^{(*)}\mathcal{P}(U') = \operatorname*{colim}_{U, U' \longrightarrow f(U)} \mathcal{P}(U)$$

où la colimite porte sur la catégorie des $U' \longrightarrow f(U)$ avec U objet de $\mathcal{C}$, les morphismes étant les $f(U_1) \xrightarrow{f(\varphi)} f(U_2)$ compatibles à $U' \longrightarrow f(U_1)$ et $U' \longrightarrow f(U_2)$.
Il est alors clair qu'un morphisme de préfaisceaux $\mathcal{P} \longrightarrow f_{(*)}\mathcal{Q}'$ induit un morphisme de préfaisceaux $f^{(*)}\mathcal{P} \longrightarrow \mathcal{Q}'$ et inversement.
L'exactitude de $f_{(*)}$ se vérifie facilement : si $\mathcal{P}'_1 \longrightarrow \mathcal{P}'_2 \longrightarrow \mathcal{P}'_3$ est exacte, alors $f_{(*)}\mathcal{P}'_1 \longrightarrow f_{(*)}\mathcal{P}'_2 \longrightarrow f_{(*)}\mathcal{P}'_3$

aussi car en tout U c'est la suite $\mathcal{P}'_1(f(U)) \longrightarrow \mathcal{P}'_2(f(U)) \longrightarrow \mathcal{P}'_3(f(U))$. L'adjoint à gauche est bien exact à droite et enfin, si $f^{(*)}$ est exact, et $\mathcal{I}'$ est injectif, alors on a un isomorphisme fonctoriel en $\mathcal{X}$:

$$\mathrm{Hom}(\mathcal{X}, f_{(*)}\mathcal{I}') \cong \mathrm{Hom}(f^{(*)}\mathcal{X}, \mathcal{I}')$$

qui est un foncteur exact en $\mathcal{X}$. □

Mentionnons d'ailleurs que le tiré en arrière d'un préfaisceau représentable est toujours représentable.

Proposition 1.1.3.3. *Soit $f : \mathcal{C} \longrightarrow \mathcal{C}'$ un foncteur entre catégories et soit Z un objet de $\mathcal{C}$. Notons h_Z le foncteur représentable $U \mapsto \mathrm{Hom}(U, Z)$ sur $\mathcal{C}$. On a alors un isomorphisme canonique de préfaisceaux sur $\mathcal{C}'$:*

$$f^{(*)}h_Z \cong h_{f(Z)}.$$

Démonstration. Il s'agit de montrer que, pour tout U' dans $\mathcal{C}'$, on a :

$$\mathrm{Hom}(U', f(Z)) \cong \operatorname*{colim}_{U, U' \longrightarrow f(U)} \mathrm{Hom}(U, Z)$$

naturellement en U'. En effet, on a un morphisme $\mathrm{Hom}(U, Z) \longrightarrow \mathrm{Hom}(U', f(Z))$ pour tout U et toute flèche $U' \longrightarrow f(U)$ qui est naturel en U et donc donne un morphisme :

$$\operatorname*{colim}_{U, U' \longrightarrow f(U)} \mathrm{Hom}(U, Z) \longrightarrow \mathrm{Hom}(U', f(Z)).$$

Dans l'autre sens, on associe à toute flèche $g \in \mathrm{Hom}(U', f(Z))$ l'élément $\mathrm{id}_Z \in \mathrm{Hom}(Z, Z)$ que l'on envoie ensuite dans $\operatorname*{colim}_{U, U' \longrightarrow f(U)} \mathrm{Hom}(U, Z)$ via la flèche canonique, en prenant $U = Z$. On vérifie alors facilement que ces flèches sont inverses l'une de l'autre. □

1.1.4 Poussé en avant et tiré en arrière au niveau des faisceaux

La discussion précédente s'adapte au niveau des faisceaux sur un site, cependant le foncteur de tiré en arrière n'est plus le même, il faut encore faisceautiser pour l'obtenir. Précisons tout cela. Soit $f : \mathcal{C} \longrightarrow \mathcal{C}'$ un morphisme de sites de Grothendieck. On commence par observer que si $\mathcal{F}'$ est un faisceau sur $\mathcal{C}'$, alors $f_{(*)}\mathcal{F}'$ est déjà un faisceau sur $\mathcal{C}$, et on pose alors :

$$f_*\mathcal{F}' = f_{(*)}\mathcal{F}'.$$

Pour ce qui est du tiré en arrière, la situation n'est pas aussi simple, et on définit le tiré en arrière d'un faisceau $\mathcal{F}$ sur $\mathcal{C}$ comme le faisceautisé de son tiré en arrière au sens des préfaisceaux :

$$f^*\mathcal{F} = \left(f^{(*)}\mathcal{F}\right)^s.$$

On dispose alors d'une paire d'adjoints avec des propriétés intéressantes.

Proposition 1.1.4.1. *Le foncteur f^* est adjoint à gauche du foncteur f_*. De plus, le foncteur f_* est exact à gauche et le foncteur f^* est exact à droite. Si f^* est exact, comme ce sera souvent le cas dans les situations géométriques, alors f_* envoie les injectifs sur les injectifs.*

Démonstration. On a, pour tout faisceaux $\mathcal{F}$ et $\mathcal{F}'$ sur $\mathcal{C}$ et $\mathcal{C}'$:

$$\mathrm{Hom}(f^*\mathcal{F},\mathcal{F}') = \mathrm{Hom}((f^{(*)})^s\mathcal{F},\mathcal{F}') = \mathrm{Hom}(f^{(*)}\mathcal{F},\mathcal{F}') = \mathrm{Hom}(\mathcal{F},f_{(*)}\mathcal{F}') = \mathrm{Hom}(\mathcal{F},f_*\mathcal{F}').$$

Par l'adjonction, on obtient que f_* est exact à gauche et que f^* est exact à droite. Le reste se prouve comme dans le cas des préfaisceaux en utilisant l'adjonction. □

Le foncteur f_* étant seulement exact à gauche, il est intéressant d'étudier les foncteurs R^nf_* : $\mathrm{Sh}(\mathcal{C}') \longrightarrow \mathrm{Sh}(\mathcal{C})$. En considérant la composée de foncteurs additifs :

$$f_* = \left(\mathrm{Sh}(\mathcal{C}') \xrightarrow{i} \mathrm{PSh}(\mathcal{C}') \xrightarrow{f_{(*)}} \mathrm{PSh}(\mathcal{C}) \xrightarrow{s} \mathrm{Sh}(\mathcal{C})\right)$$

avec $s \circ f_{(*)}$ qui est exact et i exact à gauche, on obtient :

$$R^nf_*\mathcal{F}' \cong \left(f_{(*)}R^ni\mathcal{F}'\right)^s = \left(f_{(*)}\mathcal{H}^n(\mathcal{F}')\right)^s.$$

naturellement en $\mathcal{F}'$ faisceau sur $\mathcal{C}'$. On a donc montré la proposition suivante.

Proposition 1.1.4.2. *Soit $\mathcal{C} \xrightarrow{f} \mathcal{C}'$ un morphisme de sites de Grothendieck et $\mathcal{F}'$ un faisceau sur $\mathcal{C}'$. Alors $R^nf_*\mathcal{F}'$ est (naturellement isomorphe à) la faisceautisation du préfaisceau $U \mapsto H^n(f(U),\mathcal{F}')$.*

Le résultat suivant est crucial dans beaucoup de contextes.

Théorème 1.1.4.3. *(Suite spectrale de Leray)*
Soient $\mathcal{C} \xrightarrow{f} \mathcal{C}' \xrightarrow{g} \mathcal{C}''$ des morphismes de sites de Grothendieck. Pour tout faisceau $\mathcal{F}''$ sur $\mathcal{C}''$, on dispose d'une suite spectrale, dite de Leray :

$$R^qf_*(R^pg_*\mathcal{F}'') \implies R^{p+q}(gf)_*\mathcal{F}''.$$

Ceci est encore un cas particulier du théorème de Grothendieck sur l'existence de suites spectrales associées à des composées de foncteurs additifs. Ici, il faut tout de même vérifier que le poussé en avant d'un injectif est acyclique pour le poussé en avant qui suit. Cela se fait par la théorie des faisceaux flasques (voir [28] pour les détails).
Le corollaire suivant s'obtient en choisissant $\mathcal{C} = \{*\}$ le site terminal défini dans l'exemple 1.1.1.3.

Corollaire 1.1.4.4. *Soient $\mathcal{C} \xrightarrow{f} \mathcal{C}'$ un morphisme de sites de Grothendieck. Pour tout faisceau $\mathcal{F}'$ sur $\mathcal{C}'$, on dispose d'une suite spectrale :*

$$H^q(U,(R^pf_*\mathcal{F}')) \implies H^{p+q}(f(U),\mathcal{F}').$$

1.1.5 Topologies noéthériennes et colimites de faisceaux

On mentionne enfin un point technique qui sera utile à plusieurs reprises pour calculer la cohomologie d'une colimite de faisceaux. La catégorie des préfaisceaux sur une catégorie possède toutes les (petites) colimites, et celles-ci sont calculées point par point. Si $\mathcal{C}$ est un suite, la catégorie des faisceaux sur $\mathcal{C}$ possède également toutes les (petites) colimites, et ces dernières s'obtiennent comme faisceautisation des colimites dans la catégorie des préfaisceaux.
Une question naturelle est de savoir sous quelles conditions les colimites commutent à la cohomologie. Pour cela, on introduit la notion de *site noéthérien*, qui généralise la notion d'espace topologique noéthérien.

Définition 1.1.5.1. *(Site noéthérien) Un site $\mathcal{C}$ est noéthérien si tout objet U de $\mathcal{C}$ est quasi-compact, au sens où, de tout recouvrement de U, on peut extraire un recouvrement fini.*

On trouvera alors dans [28] la preuve de l'énoncé suivant.

Théorème 1.1.5.2. *Soit $\mathcal{C}$ un site noéthérien et U un objet de $\mathcal{C}$, et soit $\mathcal{I}$ une catégorie pseudo-filtrée, au sens où pour toutes flèches $i \longrightarrow j$ et $i \longrightarrow j'$, il existe deux flèches $j \longrightarrow k$ et $j' \longrightarrow k$ qui complètent ces deux flèches en un carré commutatif, et pour toute paire de flèches parallèles, il existe une flèche qui les égalise. Alors pour tout $n \geq 0$, les foncteurs $H^n(U, \bullet)$ et $\operatorname{colim}_{\mathcal{I}}$ commutent. Autrement dit, on a un isomorphisme canonique en le diagramme de faisceaux $(\mathcal{F}_i)_{i\in\mathcal{I}}$:*

$$\operatorname{colim} H^n(U, \mathcal{F}_i) \cong H^n(U, \operatorname{colim} \mathcal{F}_i).$$

Ce théorème s'applique en particulier aux espaces topologiques noéthériens, et donc à la cohomologie de Zariski sur les schémas dont l'espace sous-jacent est noéthérien.

1.1.6 Premier groupe de cohomologie et torseurs

Soit $\mathcal{C}$ un site de Grothendieck ayant un objet terminal T et $\mathcal{F}$ un faisceau sur $\mathcal{C}$. On peut interpréter le groupe $H^1(T, \mathcal{F})$, comme paramétrant les *torseurs* sous le faisceau abélien $\mathcal{F}$. Définissons d'abord ce qu'est un torseur :

Définition 1.1.6.1. *(Torseur sous un faisceau de groupes) Un torseur (à gauche) $\mathcal{X}$ sous un faisceau de groupes $\mathcal{G}$ est un faisceau d'ensembles sur le site $\mathcal{C}$, muni d'une action de $\mathcal{G}$, c'est à dire d'un morphisme de faisceaux :*

$$\mathcal{G} \times \mathcal{X} \longrightarrow \mathcal{X}$$

qui en tout U objet de $\mathcal{C}$ soit une action de groupe, et telle qu'il existe un recouvrement (U_i) de T tel que $\mathcal{X}_{|U_i}$, vu comme faisceau sur le site des objets de $\mathcal{C}$ au dessus de U_i et muni de l'action du faisceau $\mathcal{G}_{|U_i}$, soit isomorphe en tant que faisceau muni d'une action de $\mathcal{G}_{|U_i}$ au faisceau $\mathcal{G}_{|U_i}$, on dit alors que $\mathcal{X}$ est trivial sur U_i, ou que $\mathcal{X}_{|U_i}$ est trivial.

On peut donner une définition équivalente plus agréable à manipuler.

Proposition 1.1.6.2. *Soit $\mathcal{X}$ un faisceau d'ensembles sur le site $\mathcal{C}$ muni d'une action de $\mathcal{G}$. Alors $\mathcal{X}$ est un torseur si et seulement si pour tout objet U de $\mathcal{C}$ tel que $\mathcal{X}(U) \neq \emptyset$, l'action de $\mathcal{G}(U)$ sur $\mathcal{X}(U)$ est simplement transitive, et il existe un recouvrement (U_i) de l'objet terminal tel que $\mathcal{X}(U_i) \neq \emptyset$.*

Démonstration. Il est clair qu'un torseur vérifie cette condition. Supposons à présent que $\mathcal{X}$ vérifie cela et montrons que c'est un torseur. On choisit (U_i) un recouvrement de l'objet terminal T tel que $\mathcal{X}(U_i) \neq \emptyset$. On choisit alors $s_i \in \mathcal{X}(U_i)$ et on considère pour chaque $Z \xrightarrow{f} U_i$ au dessus de U_i, l'application :

$$\eta_Z : \mathcal{G}(Z) \longrightarrow \mathcal{X}(Z)$$

qui à g associe $g(s_i)_{|Z}$. Ceci donne un morphisme de faisceaux $\mathcal{G}_{|U_i} \longrightarrow \mathcal{X}_{|U_i}$ sur le site des objets au dessus de U_i, compatible à l'action de $\mathcal{G}_{|U_i}$. Il reste à voir que c'est un isomorphisme : soit $Z \xrightarrow{f} U_i$ au dessus de U_i. On a $\mathcal{X}(Z) \neq \emptyset$ car $(s_i)_{|Z} \in \mathcal{X}(Z)$, et l'action de $\mathcal{G}(Z)$ sur $\mathcal{X}(Z)$ est simplement transitive, donc η_Z est une bijection. □

Si $\mathcal{F}$ est un faisceau de groupes abéliens, on peut alors paramétrer les torseurs à isomorphisme près par le groupe $H^1(T,\mathcal{F})$.

Théorème 1.1.6.3. *Soit $\mathcal{C}$ un site avec un objet terminal T (par exemple le site des objets au dessus d'un objet U d'un site $\mathcal{C}'$) et soit $\mathcal{F}$ un faisceau de groupes abéliens sur $\mathcal{C}$. On dispose d'une bijection canonique entre les éléments de $H^1(T,\mathcal{F})$ et les torseurs sous $\mathcal{F}$ à isomorphisme près.*

Démonstration. Puisque $H^1(T,\mathcal{F}) \cong \check{H}^1(T,\mathcal{F})$ (voir 1.1.2.4), on travaille avec la cohomologie à la Čech. Soit (U_i) un recouvrement de T.
Soit $\mathcal{X}$ un torseur *trivialisé* par ce recouvrement. Autrement dit, on dispose pour tout i d'un isomorphisme :

$$\varphi_i : \mathcal{X}_{|U_i} \longrightarrow \mathcal{F}_{|U_i}$$

compatible à l'action de $\mathcal{F}_{|U_i}$. Ceci donne, pour tous i,j, un isomorphisme :

$$g_{ij} : \mathcal{F}_{|U_{ij}} \xrightarrow{\varphi_i^{-1}} \mathcal{X}_{|U_{ij}} \xrightarrow{\varphi_j} \mathcal{F}_{|U_{ij}}$$

compatible à l'action de $\mathcal{F}_{|U_{ij}}$, et un tel isomorphisme est donné par la translation par une section sur U_{ij}, que l'on note h_{ij}, à savoir l'image de la section nulle. Ces morphismes g_{ij}, appelés *cocycles*, vérifient la relation de cocycle :

$$g_{jk}g_{ij} = g_{ik}.$$

En dépliant la définition de $\check{H}^1((U_i),\mathcal{F})$, on voit alors que (h_{ij}) définit un élément de $\check{H}^1((U_i),\mathcal{F})$ (ou du moins sa classe définit un tel élément).
Il reste alors quelques détails à vérifier : deux torseurs isomorphes donnent la même classe de cohomologie à la Čech et toute classe de cohomologie à la Čech donne un torseur bien défini. On se convainc alors que le groupe $\check{H}^1((U_i),\mathcal{F})$ paramètre les torseurs sous $\mathcal{F}$ trivialisés par le recouvrement (U_i) à isomorphisme près. De là, en passant à la colimite, on en déduit le théorème. □

Remarque 1.1.6.4. (Premier groupe de cohomologie non abélienne)
Si $\mathcal{G}$ est un faisceau en groupes, il est toujours possible de définir l'ensemble $\check{H}^1((U_i),\mathcal{G})$ (et donc, en prenant la colimite sur les recouvrements de U, de $\check{H}^1(U,\mathcal{G})$) avec la définition combinatoire des cocycles modulo une certaine relation d'équivalence. Plus précisément, un cocycle pour le recouvrement (U_i) est la donnée de $h_{ij} \in \mathcal{G}(U_{ij})$ qui vérifient :

$$h_{jk}h_{ij} = h_{ik}$$

sur U_{ijk}, et deux cocycles (h_{ij}) et (h'_{ij}) sont équivalents s'il existe des $u_i \in \mathcal{G}(U_i)$ tels que pour tous i,j on ait :

$$h'_{ij} = u_i h_{ij} u_j^{-1}$$

sur U_{ij}. Par le même argument, on obtient alors que, si T est un objet terminal de $\mathcal{C}$, $\check{H}^1(T,\mathcal{G})$ paramètre les $\mathcal{G}$-torseurs à isomorphisme près.
Cependant on fera attention au fait que $\check{H}^1(U,\mathcal{G})$ est un ensemble pointé (le point particulier étant le cocycle trivial) et non un groupe.

Un cas intéressant de $\check{H}^1(T,\mathcal{G})$ est quand $\mathcal{G}$ est le groupe d'automorphismes d'un faisceau $\mathcal{F}$. En effet, cet ensemble pointé paramètre alors les *formes tordues* du faisceau $\mathcal{F}$, c'est à dire les faisceaux localement isomorphes à $\mathcal{F}$. On commence par donner une version très simple avec des faisceaux d'ensembles pour donner l'idée de ce qui est en fait une philosophie très générale.

Théorème 1.1.6.5. *Soit $\mathcal{C}$ un site avec un objet terminal T et soit $\mathcal{F}$ un faisceau d'ensembles sur le site $\mathcal{C}$. On considère le faisceau de groupes $\underline{\mathrm{Aut}}(\mathcal{F})$ défini par :*

$$\underline{\mathrm{Aut}}(\mathcal{F})(U) = \mathrm{Aut}_{\mathrm{Sh}(\mathcal{C}/U,\mathrm{Set})}(\mathcal{F}_{|U})$$

avec $\mathcal{C}/U$ le site des objets de $\mathcal{C}$ au dessus de U. L'ensemble pointé $\check{H}^1(T,\underline{\mathrm{Aut}}(\mathcal{F}))$ paramètre alors les faisceaux d'ensembles $\mathcal{G}$ localement isomorphes à $\mathcal{F}$, au sens où il existe un recouvrement de l'objet terminal par des objets U_i tels que $\mathcal{G}_{|U_i}$ soit isomorphe à $\mathcal{F}_{|U_i}$ dans la catégorie $\mathrm{Sh}(\mathcal{C}/U_i,\mathrm{Set})$ des faisceaux à valeurs ensemblistes sur le site au dessus de U_i, à isomorphisme près.

Démonstration. Il suffit de raisonner avec les cocycles : on montre d'abord que $\check{H}^1((U_i),\underline{\mathrm{Aut}}(\mathcal{F}))$ paramètre les faisceaux qui sont isomorphes à $\mathcal{F}$ sur chaque objet U_i. Dans un sens, on remarque que si (h_{ij}) est un cocycle, on peut l'utiliser pour recoller les faisceaux $\mathcal{F}_{|U_i}$ en un faisceau $\mathcal{F}'$ localement isomorphe à $\mathcal{F}$. Dans l'autre sens, si $\mathcal{F}'$ est isomorphe à $\mathcal{F}$ sur chaque objet U_i, on a des isomorphismes $\mathcal{F}'_{|U_i} \longrightarrow \mathcal{F}_{|U_i}$ qui donnent des cocycles en les comparant sur deux objets différents. □

Le théorème 1.1.6.5 est un cas particulier d'une philosophie plus générale ou l'on peut considérer un faisceau $\mathcal{F}$ à valeurs dans une catégorie qui varie sur le site. Une formulation générale serait assez compliquée, pour une preuve qui est de toute façon exactement la même, donc mentionnons simplement un autre cas particulier intéressant.
Si $\mathcal{C}$ est un site et si $\mathcal{O}$ est un faisceau d'anneaux sur le site $\mathcal{C}$, un faisceau de $\mathcal{O}$-modules sur $\mathcal{C}$ est un faisceau de groupes abéliens $\mathcal{A}$ tel que chaque $\mathcal{A}(U)$ est muni d'une structure de $\mathcal{O}(U)$ module de façon compatible aux restrictions.

Théorème 1.1.6.6. *Soit $\mathcal{C}$ un site avec un objet terminal T muni d'un faisceau d'anneaux $\mathcal{O}$ et soit $\mathcal{F}$ un faisceau de $\mathcal{O}$-modules sur le site $\mathcal{C}$. On considère le faisceau de groupes $\underline{\mathrm{Aut}}_{\mathcal{O}}(\mathcal{F})$ défini par :*

$$\underline{\mathrm{Aut}}_{\mathcal{O}}(\mathcal{F})(U) = \mathrm{Aut}_{\mathcal{O}_{|U}-\mathrm{Mod}}(\mathcal{F}_{|U})$$

L'ensemble pointé $\check{H}^1(T,\underline{\mathrm{Aut}}_{\mathcal{O}}(\mathcal{F}))$ paramètre alors les faisceaux de $\mathcal{O}$-modules $\mathcal{G}$ localement isomorphes à $\mathcal{F}$.

On va à présent appliquer le cadre unificateur des sites à des situations géométriques et algébriques.

1.2 Cohomologie des groupes

La cohomologie des groupes est un cas particulier très élémentaire de cohomologie des faisceaux sur un site. Pour ce qui est des groupes discrets (non-munis d'une topologie), on considère la catégorie $G-\mathrm{Set}$ des G-ensembles à gauche et on la munit de la topologie canonique définie en 1.1.1.3. La proposition suivante est alors élémentaire :

Proposition 1.2.0.1. *Soit G un groupe. On a une équivalence de catégories :*

$$G-\mathrm{Mod} \simeq \mathrm{Sh}(G-\mathrm{Set})$$

via le plongement de Yoneda, et dans l'autre sens, via $\mathcal{F} \mapsto \mathcal{F}(G)$, en munissant $\mathcal{F}(G)$ de l'action suivante : si $s \in \mathcal{F}(G)$ et $g \in G$, on pose $gs = \mathcal{F}(R_g)(s)$ avec $\_g : G \mapsto G$ la translation à droite par G.

Via cette identification, si A est un G-module, et si $h_A = \mathrm{Hom}(\bullet, A)$ est le faisceau associé et $\{*\}$ est le point muni de l'action triviale de G, alors on a :

$$h_A(\{*\}) = \mathrm{Hom}(\{*\}, A) = A^G$$

qui est le groupe des points fixes de A. En particulier, on retrouve la cohomologie des groupes, définie en prenant le foncteur dérivé des points fixes :

$$H^n(G, A) = H^n(\{*\}, h_A)$$

via cette équivalence de catégories.
Dans les situations qui nous intéressent, les groupes qui vont apparaître sont des groupes de Galois d'extensions souvent infinies, et ces groupes sont munis de topologies. Dans ce cas, on définit la cohomologie d'une façon un peu différente.

1.2.1 Quelques mots sur les groupes profinis

Commençons par un bref rappel sur les groupes profinis. Les groupes profinis sont les limites projectives de groupes finis. Ils apparaissent naturellement en théorie de Galois à travers les groupes de Galois des extensions de corps.

Définition 1.2.1.1. *Un ensemble profini est un espace topologique compact (i.e. quasi-compact et séparé) totalement discontinu. La catégorie des ensembles profinis, notée ici* PSet, *est la sous-catégorie pleine de la catégorie des espaces topologiques dont les objets sont les ensembles profinis. Cette catégorie possède toutes les petites limites.*
De façon alternative, on peut définir un ensemble profini comme une limite projective d'ensembles finis, chacun muni de la topologie discrète (la limite est alors munie de la topologie limite).
Un groupe profini est un groupe topologique dont l'espace topologique sous-jacent est profini. Ils forment une catégorie PGrp *qui possède également toutes les petites limites.*

Les ensembles profinis possèdent une base de voisinages ouverts et fermés, et si G est un groupe profini, les sous-groupes ouverts distingués forment une base de voisinages de l'élément neutre. Par compacité, chacun de ces sous-groupes est d'indice fini, et le morphisme canonique :

$$G \longrightarrow \lim_U G/U$$

avec $U \subseteq G$ sous-groupe ouvert distingué, est un isomorphisme de groupes topologiques. Ceci permet de définir alternativement les groupes profinis comme limites projectives de groupes finis, chacun muni de la topologie discrète.
Le foncteur d'oubli PGrp $\longrightarrow$ Grp qui à un groupe profini associe le groupe sous-jacent possède un adjoint, appelé *complétion profinie*, construit de la façon suivante : à tout groupe G, on associe sa complétion profinie, qui est le groupe profini :

$$\mathrm{Prof}(G) = \lim_H G/H$$

avec H sous-groupe distingué d'indice fini de G.
Par exemple, la complétion profinie de $\mathbb{Z}$ est le groupe $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. On fera attention à ce que la complétion profinie de la complétion profinie n'est pas toujours isomorphe à la complétion profinie : ceci est dû au fait qu'il existe des groupes profinis qui possèdent des sous-groupes distingués d'indice fini qui ne sont pas ouverts (et donc pas fermés).

Définition 1.2.1.2. *Soit L/K une extension galoisienne de corps. On munit le groupe de Galois* $\mathrm{Gal}(L/K)$ *de la topologie de Krull dont une base de voisinages de l'identité est donnée par les sous-groupes* $\mathrm{Gal}(L/E)$ *avec $L/E/K$ une extension intermédiaire et $[E:K]<\infty$. Autrement dit, deux éléments $\sigma,\tau\in\mathrm{Gal}(L/K)$ sont proches s'il existe une grande extension finie de K, E, telle que $\sigma_{|E}=\tau_{|E}$.*

Avec cette définition, on obtient un isomorphisme de groupes topologiques :

$$\mathrm{Gal}(L/K)\cong\lim_{E}\mathrm{Gal}(E/K)$$

avec E/K une extension finie galoisienne contenue dans L. Le groupe de Galois de L/K est donc un groupe profini.
La correspondance de Galois se généralise alors en faisant correspondre les sous-groupes *fermés* de $\mathrm{Gal}(L/K)$ avec les extensions intermédiaires via $H\mapsto L^H$ et $E\mapsto\mathrm{Gal}(L/E)$. Les sous-groupes *ouverts* correspondent alors aux extensions finies de K contenues dans L. La topologie de Krull est naturelle en l'extension : si E est une extension intermédiaire de K, alors les topologies induites et de Krull sur $\mathrm{Gal}(L/E)$ coïncident, et pareil avec les topologies quotient et de Krull sur $\mathrm{Gal}(E/K)$ si E/K est galoisienne.

Définition 1.2.1.3. *À tout corps K, on associe son groupe de Galois absolu, défini comme le groupe de Galois de K_s/K avec K_s une clôture séparable de K.*

Par exemple, le groupe de Galois absolu d'un corps fini est isomorphe à $\hat{\mathbb{Z}}$, il est topologiquement engendré par le Frobenius, c'est à dire que le sous-groupe engendré par le Frobenius est dense.

Définition 1.2.1.4. *(Indice d'un sous-groupe, ordre d'un groupe profini et pro-p-groupes)*
Soit G un groupe profini et H un sous-groupe fermé de G. On définit l'indice $[G:H]$ via la formule suivante :

$$[G:H]=\operatorname*{ppcm}_{U}\frac{[G:U]}{[HU:U]}$$

le ppcm *portant sur les sous-groupes ouverts normaux de G. Ce* ppcm *est à valeurs dans $\prod_p(\mathbb{N}\cup\{\infty\})$. On définit aussi l'ordre de G comme $|G|=[G:1]$.*
Si p est un nombre premier, un pro-p-groupe est un groupe profini dont l'ordre est une puissance (éventuellement infinie) de p. De façon équivalente, tout sous-groupe d'indice fini est d'indice une puissance de p.
Si G est un groupe profini, on appelle pro-p-Sylow tout sous-pro-p-groupe (fermé) maximal de G.

Par exemple, $\left|\mathbb{Z}_p\right|=p^\infty$. On dispose d'une formule de multiplicativité pour l'indice des groupes profinis. La théorie de Sylow usuelle s'adapte très facilement au cas des groupes profinis.

Théorème 1.2.1.5. *(Théorie de Sylow profinie)*
Soit G un groupe profini. Tout pro-p-sous-groupe de G est contenu dans un pro-p-Sylow, en particulier G possède un pro-p-Sylow, et deux pro-p-Sylow sont conjugués. De plus, si H est un pro-p-Sylow de G, alors $p\nmid[G:H]$.

La cohomologie des groupes profinis s'inscrit dans le cadre général de la cohomologie des faisceaux. Pour cela, fixons G un groupe profini et considérons la catégorie $G-\mathrm{Set}^{\mathrm{top}}$ des G-ensembles topologiques, c'est à dire des ensembles X munis d'une action (à gauche) de G qui soit continue pour la topologie discrète. De façon équivalente, on demande que tout stabilisateur pour cette action soit un sous-groupe ouvert de G, ou encore que X soit la réunion des X^U avec U sous-groupe ouvert distingué de G. On munit cette catégorie de la topologie canonique définie dans l'exemple 1.1.1.3, de

façon à obtenir un site, toujours noté $G-\mathrm{Set}^{\mathrm{top}}$. On vérifie facilement qu'un recouvrement $(U_i \xrightarrow{f_i} U)$ pour cette topologie est une famille de morphismes de G-ensembles tels que $U = \bigcup_i f_i(U_i)$. On a alors la proposition suivante.

Proposition 1.2.1.6. *Soit G un groupe. On a une équivalence de catégories :*

$$G-\mathrm{Mod}^{\mathrm{top}} \simeq \mathrm{Sh}(G-\mathrm{Set}^{\mathrm{top}})$$

entre la catégorie des G-modules topologiques, c'est à dire des G-modules qui sont topologiques en tant que G-ensemble, et la catégorie des faisceaux sur le site $G-\mathrm{Set}^{\mathrm{top}}$. L'équivalence de catégorie est donnée par le foncteur de Yoneda, comme dans 1.2.0.1, et dans l'autre sens par :

$$\mathcal{F} \mapsto \operatorname*{colim}_U \mathcal{F}(G/U)$$

avec U sous-groupe ouvert distingué de G.

Via cette identification, si A est un G-module topologique, et si $h_A = \mathrm{Hom}(\bullet, A)$ est le faisceau associé et $\{*\}$ est le point muni de l'action triviale de G, alors on a toujours :

$$h_A(\{*\}) = \mathrm{Hom}(\{*\}, A) = A^G$$

qui est le groupe des points fixes de A. Ainsi, comme pour les groupes abstraits, on retrouve la cohomologie des groupes profinis définie en prenant le foncteur dérivé des points fixes :

$$H^n(G, A) = H^n(\{*\}, h_A)$$

via cette équivalence de catégories. On utilisera la même notation que pour la cohomologie des groupes abstraits, en sous-entendant que si G est un groupe profini cette notation désigne la cohomologie des groupes profinis.
On peut d'ailleurs en donner une description plus explicite en terme de cocycles, ce qui sera bien utile.

Théorème 1.2.1.7. *Soit G un groupe profini et A un G-module topologique. On définit le groupe $C^n(G, A)$ des applications continues de G^n vers A, avec A muni de la topologie discrète, et on définit un complexe $C^\bullet(G, A)$ de groupes abéliens via la formule suivante :*

$$d(f)(g_1, \ldots, g_{n+1}) = g_1 f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

On a alors des isomorphismes fonctoriels entre la cohomologie du G-module topologique A et la cohomologie du complexe $C^\bullet(G, A)$.

La cohomologie des groupes profinis peut aussi être définie comme une extension de la cohomologie des groupes finis, grâce au fait suivant.

Proposition 1.2.1.8. *Soit G un groupe profini et A un G-module topologique. On a alors des isomorphismes canoniques compatibles aux morphismes de bord :*

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

et :

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

avec la colimite qui porte sur les sous-groupes ouverts distingués de G. Ici, A^U désigne le groupe des points de A fixés par U.

Démonstration. Pour tout U, on a un morphisme naturel :

$$C^n(G/U, A^U) \longrightarrow C^n(G, A)$$

qui envoie $(G/U)^n \longrightarrow A^U$ sur $G^n \longrightarrow (G/U)^n \longrightarrow A^U \longrightarrow A$. Ce morphisme est compatible aux flèches $i \mapsto j$ dans $\mathcal{I}$ et donne donc un morphisme :

$$\mathrm{colim}_U\, C^n(G/U, A^U) \longrightarrow C^n(G, A)$$

qui est clairement compatible aux morphismes de bords. Ensuite, si $f \in C^n(G, A)$, l'image de f est finie car G est compact et A est discret. Ainsi l'image de f atterit dans un A^U car A est la réunion filtrée de ces sous-modules ci, et f se factorise par un $(G/U)^n$ avec U sous-groupe distingué ouvert de G.
Ceci montre la surjectivité de ce morphisme. Il est aussi injectif car si $f : (G/U)^n \longrightarrow A^U$ devient nul comme morphisme $G^n \longrightarrow A$, il était initialement nul.
Ainsi, on a un isomorphisme de complexes de cochaînes :

$$\mathrm{colim}_U\, C^*\left(G/U, A^U\right) \cong C^*(G, A).$$

On conclut alors en utilisant le fait que les colimites filtrantes commutent à la cohomologie des complexes. □

En conséquence, comme les $H^n(G/U, A^U)$ avec $n \geq 1$ sont des groupes abéliens de torsion (tués par $|G/U|$), le groupe $H^n(G, A)$ est de torsion.
Un cas important de calcul de cohomologie est celui du $H^1(G, A)$ avec A muni de l'action triviale de G, c'est à dire l'action qui fixe tout. Dans ce cas, on a :

$$H^1(G, A) = \mathrm{Hom}(G, A)$$

où ici $\mathrm{Hom}(G, A)$ désigne l'ensemble des morphismes de groupes continus de G dans A.

La cohomologie des groupes profinis commute aux colimites filtrantes.

Proposition 1.2.1.9. *Soit G un groupe profini, $\mathcal{I}$ une catégorie pseudo-filtrée et $(A_i)_{i\in\mathcal{I}}$ un diagramme de G-modules topologiques. On a alors un isomorphisme canonique :*

$$\mathrm{colim}_i\, H^n(G, A_i) \cong H^n(G, \mathrm{colim}_i\, A_i).$$

L'idée de la preuve est la suivante : le site $G - \mathrm{Set}^{\mathrm{top}}$ n'est peut-être pas directement noéthérien, mais sa catégorie de faisceaux est équivalente à la catégorie des faisceaux sur le site $G - \mathrm{Set}^{\mathrm{top,fin}}$ des G-ensembles topologiques *finis*, qui lui est noéthérien, et on peut alors appliquer 1.1.5.2. On renvoie encore à [28], exemple 3.9.4 pour les détails.

1.2.2 Torseurs en cohomologie des groupes

Le théorème de classification des torseurs 1.1.6.3 donne le résultat suivant pour la cohomologie des groupes profinis.

Théorème 1.2.2.1. *Soit G un groupe profini et A un G-module topologique. Le groupe $H^1(G,A)$ classifie les ensembles non-vides X munis d'une action de G et d'une action de A avec la compatibilité suivante :*

$$g*(ax) = (g*a)(g*x)$$

pour tous $g \in G$, $a \in A$ et $x \in X$, tels que pour tout sous-groupe ouvert U de G, ou bien X^U est vide, ou bien l'action de A^U sur X^U est simplement transitive, le tout à isomorphisme de ces structures ci près.

Démonstration. Le théorème 1.1.6.3 montre que $H^1(G,A) = H^1(\{*\}, h_A)$ classifie les torseurs sous le faisceau h_A sur le site $G - \mathrm{Set}^{\mathrm{top}}$ à isomorphisme près. Il s'agit donc de comprendre ces objets là. Premièrement, un tel torseur est un faisceau $\mathcal{X}$, nécessairement représentable par un G-ensemble topologique X car tous les faisceaux sur ce site sont représentables (c'est la même preuve que 1.2.1.6), muni d'une action de h_A, ce qui revient par Yoneda à une action :

$$A \times X \longrightarrow X$$

compatible à l'action de G. Il reste à traduire ce que signifie être un torseur à présent. Cela signifie deux choses :

— Il existe un recouvrement (Y_i) de l'objet terminal $\{*\}$ pour lequel $h_X(Y_i) \neq \emptyset$ pour tout i. Dire que c'est un recouvrement de l'objet terminal revient à dire que l'un des Y_i est non-vide, et $h_X(Y_i) = \mathrm{Hom}(Y_i, X) = \prod_O \mathrm{Hom}(O, X)$ où le produit porte sur les orbites de Y_i sous l'action de G. Ainsi, on peut supposer l'action transitive sur Y_i, et donc ce premier point est équivalent à ce qu'il existe U un sous-groupe ouvert de G tel que :

$$X^U = \mathrm{Hom}_G(G/U, X) \neq \emptyset.$$

Or, si X est non-vide, n'importe quel point $x \in X$ possède un stabilisateur ouvert car l'action est continue et donc il existe U sous-groupe ouvert de G tel que X^U est non-vide. Cette condition revient donc simplement à ce que X soit non-vide.

— Pour tout G-ensemble topologique Z tel que $h_X(Z) \neq \emptyset$, l'action de $h_A(Z)$ sur $h_X(Z)$ est simplement transitive. Encore une fois, on se ramène aux Z qui sont transitifs, c'est à dire aux G/V avec V sous-groupe ouvert de G. On demande donc que l'action de A^V sur X^V soit simplement transitive dès que $X^V \neq \emptyset$.

□

Remarque 1.2.2.2. On peut aussi donner une version de ce théorème pour des groupes A non-commutatifs muni d'une action de G compatible, en se basant sur la remarque 1.1.6.4. On note alors $H^1(G,A)$ le premier ensemble pointé de cohomologie d'un groupe profini G agissant sur un groupe A de façon continue.

1.2.3 Coinduction

On commence par rappeler la notion de coinduction pour les groupes abstraits. L'idée est de partir de l'énoncé général suivant en théorie des modules.

Théorème 1.2.3.1. *Soit A un anneau (non-nécessairement commutatif) et B une A-algèbre. La notation $A - \mathrm{Mod}^{\ell}$ désigne la catégorie des A-modules à gauche. On dispose de foncteurs adjoints :*

$$\begin{array}{c} A - \mathrm{Mod}^{\ell} \\ \mathrm{Ind}_A^B \big\downarrow \big\uparrow \big\downarrow \mathrm{Coind}_A^B \\ B - \mathrm{Mod}^{\ell} \end{array}$$

avec $\mathrm{Ind}_A^B M = B \otimes_A M$ *et* $\mathrm{Coind}_A^B M = \mathrm{Hom}_A(B, M)$*, et la flèche du milieu est le foncteur d'oubli.*

La vérification de cet énoncé est élémentaire, et elle s'applique notamment au cas suivant.

Définition 1.2.3.2. *Soit G un groupe (abstrait) et H un sous-groupe de G. En choisissant $A = \mathbb{Z}[H]$ et $B = \mathbb{Z}[G]$ dans le théorème précédent, on obtient des foncteurs* Ind_H^G *et* Coind_H^G*, d'induction et de coinduction.*

Notons que $\mathrm{Coind}_H^G(A)$ correspond à l'ensemble des applications de G dans A qui sont H-équivariantes, et s'il on fixe un système de représentants S de G/H, on peut voir $\mathrm{Ind}_H^G(A)$ comme $\bigoplus_{s\in S} sA$. On rappelle d'ailleurs que si H est d'indice fini dans G, ces deux foncteurs sont isomorphes.
Dans le cas des groupes profinis, il est toujours possible de définir la coinduction, de la façon suivante.

Définition 1.2.3.3. *Soit G un groupe profini et H un sous-groupe fermé de G. Si A est un H-module topologique, on pose :*

$$\mathrm{Coind}_H^G(A) = \mathrm{colim}_U \mathrm{Coind}_{H/(H\cap U)}^{G/U}\left(A^{H\cap U}\right)$$

où la colimite porte sur les sous-groupes ouverts distingués de G. On vérifie alors que cet un G-module topologique et que le foncteur ainsi formé est un adjoint à droite du foncteur d'oubli. Dans le cas où H est ouvert, la colimite peut bien sûr porter sur les U contenus dans H.

Le lemme de Shapiro est alors encore valable dans le cadre cohomologique grâce à la proposition 1.2.1.8 :

Théorème 1.2.3.4. *(Lemme de Shapiro en cohomologie des groupes profinis) Soit G un groupe profini et H un sous-groupe fermé de G. Soit A un H-module topologique. On a un isomorphisme canonique :*

$$H^n(H, A) \cong H^n(G, \mathrm{Coind}_H^G(A)).$$

1.2.4 Restriction, inflation, corestriction et cup-produit

Le but de cette partie est de donner un très bref résumé des opérations usuelles de la cohomologie des groupes.

Définition 1.2.4.1. *(Restriction, inflation) Soit G un groupe profini, H un sous-groupe fermé de G, et A un G-module. On a une application naturelle de restriction $C^n(G, A) \longrightarrow C^n(H, A)$ qui induit un morphisme en cohomologie :*

$$\mathrm{Res}_H^G : H^n(G, A) \longrightarrow H^n(H, A)$$

et on notera parfois ω_H pour la restriction d'une classe de cohomologie ω à H. Au niveau du H^0, c'est l'inclusion naturelle de A^G dans A^H.
Si H est un sous-groupe fermé distingué, la même construction via le morphisme $G \longrightarrow G/H$ donne un morphisme en cohomologie, dit d'inflation :

$$\mathrm{Inf}_{G/H}^G : H^n(G/H, A^H) \longrightarrow H^n(G, A).$$

Si H est un sous-groupe ouvert de G, on peut aussi définir des morphismes de *corestriction*, $H^n(H, A) \longrightarrow H^n(G, A)$, comme en cohomologie des groupes finis.

Définition 1.2.4.2. *(Corestriction) Soit G un groupe profini et H un sous-groupe ouvert de G et soit A un G-module. On définit un morphisme G-équivariant :*

$$\mathrm{Tr} : \mathrm{Coind}_H^G(A) \longrightarrow A$$

défini comme colimite portant sur les sous-groupes distingués ouverts U contenus dans H des morphismes G/U-équivariants :

$$\mathrm{Tr}_U : \mathrm{Coind}_{H/U}^{G/U}(A^U) \longrightarrow A^U$$

qui envoient $f : G/U \longrightarrow A^U$ une application H/U-équivariante sur l'élément :

$$\sum_{s \in S_U} s f(s^{-1}) \in A^U$$

avec S_U un système de représentants de $(G/U)/(H/U)$. On vérifie aisément que la construction ne dépend pas de ces choix de systèmes de représentants et qu'ils sont bien tous compatibles en faisant varier U.
En cohomologie, le morphisme Tr *induit alors des morphismes :*

$$H^n(G, \mathrm{Coind}_H^G(A)) \longrightarrow H^n(G, A)$$

et par le lemme de Shapiro 1.2.3.4, on a donc des morphismes, dits de corestriction :

$$H^n(H, A) \overset{\mathrm{Cor}_H^G}{\longrightarrow} H^n(G, A).$$

Les morphismes de restriction, corestriction et inflation sont compatibles aux morphismes connectants dans les suites exactes longues de cohomologie, au sens où si $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ est une suite exacte de G-modules topologiques, et si on note $\nabla : H^n(C) \longrightarrow H^{n+1}(A)$ le morphisme connectant, alors ∇ commute aux différents morphismes construits lorsque cela a du sens.
Comme dans le cas des groupes finis, si H est un sous-groupe ouvert de G, on a :

$$\mathrm{Cor}_H^G \circ \mathrm{Res}_H^G = [G : H]\,\mathrm{id}.$$

On rappelle à présent la *suite spectrale de Hochschild-Serre*. Si G est un groupe profini et H un sous-groupe fermé distingué de G, et si A est un G-module, alors chaque $H^n(H, A)$ est muni d'une action continue de G/H par conjugaison. En effet, pour tout $\sigma \in G$, on a un automorphisme induit sur H par conjugaison puisque H est distingué :

$$\iota_\sigma : H \longrightarrow H$$

ainsi qu'un isomorphisme :

$$f : \sigma : A \longrightarrow A$$

qui envoie x sur $\sigma(x)$. Puisque f et ι_σ sont compatibles, f induit un isomorphisme $H^n(H, A) \longrightarrow H^n(H, A)$. C'est l'action de G sur $H^n(H, A)$, et H agit trivialement pour cette action, de sorte que l'action se factorise par G/H. On a alors les foncteurs exacts à gauche suivants :

$$G - \mathrm{Mod}^{\mathrm{top}} \overset{(\bullet)^H}{\longrightarrow} (G/H) - \mathrm{Mod}^{\mathrm{top}} \overset{(\bullet)^G}{\longrightarrow} \mathrm{Ab}$$

dont la composée donne le foncteur $(\bullet)^G$. Notons que ces morphismes viennent des morphismes de sites suivants :

$$\{*\} \longrightarrow (G/H) - \mathrm{Set}^{\mathrm{top}} \longrightarrow G - \mathrm{Set}^{\mathrm{top}}$$

donc la suite spectrale de Leray 1.1.4.3 s'applique. On pourrait aussi raisonner directement avec le théorème de Grothendieck en justifiant que le premier foncteur envoit les injectifs sur des acycliques pour le second foncteur. On a ainsi une suite spectrale dite de Hoschild-Serre :

$$H^q(G/H, H^p(H,A)) \implies H^{p+q}(G,A).$$

L'analyse des premiers termes de cette suite spectrale donne lieu aux suites exactes suivantes, dites d'inflation-restiction.

Théorème 1.2.4.3. *(Hochschild-Serre)*
Soit G un groupe profini, H un sous-groupe fermé et A un G-module. On a une suite exacte :

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G,A) \xrightarrow{\text{Res}} H^1(H,A)^{G/H} \longrightarrow H^2(G/H, A^H) \xrightarrow{\text{Inf}} H^2(G,A).$$

De plus, si $H^p(H,A) = 0$ pour tout $p \in \{1, \dots, n-1\}$, avec $n \geq 1$, alors on a aussi une suite exacte :

$$0 \longrightarrow H^n(G/H, A^H) \xrightarrow{\text{Inf}} H^n(G,A) \xrightarrow{\text{Res}} H^n(H,A)^{G/H}.$$

Le dernier outil important en cohomologie des groupes (profinis) est le *cup-produit*. Si G est un groupe profini et A et B sont deux G-modules topologiques, on peut former leur produit tensoriel $A \otimes B = A \otimes_{\mathbb{Z}} B$ qui est encore un G-module topologique et on a des morphismes :

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

Pour les construire, on se ramène au cas des groupes finis grâce à 1.2.1.8, puis on utilise la méthode de *décalage dimensionnel*, ou *dimension shifting* pour les déduire des cas simples où $p = 0$ ou $q = 0$. On renvoie au livre de Neukirch pour les détails de la construction [19] et pour des cas particuliers importants. L'essentiel pour nous est que le cup-produit est anti-commutatif en degré 1, qu'il est fonctoriel et qu'il vérifie une relation de compatibilité avec les morphismes connectants : si $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ est une suite exacte de G-modules topologiques et si D est un G-module topologique tel que la suite obtenue en tensorisant à droite par D reste exacte, alors on a :

$$\nabla(c) \cup d = \nabla(c \cup d)$$

pour $c \in H^p(G,C)$ et $d \in H^q(G,D)$, et de façon similaire en tensorisant cette fois-ci à gauche par D :

$$d \cup \nabla(c) = (-1)^q \nabla(d \cup c).$$

Chapitre 2

Cohomologie galoisienne

La cohomologie des groupes profinis s'applique directement aux groupes de Galois des extensions galoisiennes de corps. C'est ce qu'on va étudier à présent. Soit L/K une extension galoisienne de corps (non-nécessairement finie). Le groupe de Galois $\mathrm{Gal}(L/K)$ munit de la topologie de Krull est un groupe profini (voir 1.2.1.2). Si A est un $\mathrm{Gal}(L/K)$-module, on pose alors :

$$H^n(L/K, A) = H^n(\mathrm{Gal}(L/K), A)$$

pour plus de simplicité. De même, si A est un G_K-module, on pose :

$$H^n(K, A) = H^n(G_K, A)$$

de sorte que, par 1.2.1.8 :

$$H^n(K, A) = \mathrm{colim}_{L/K} H^n\left(L/K, A^{G_L}\right)$$

où la colimite porte sur les extensions finies galoisiennes L/K contenues dans K_s une clôture séparable fixée de K.
Si M est une extension intermédiaire, le foncteur de coinduction $\mathrm{Coind}_{\mathrm{Gal}(L/M)}^{\mathrm{Gal}(L/K)}$ sera noté Coind_M^K, et on adopte des notations similaires pour les morphismes de restriction, corestriction et inflation.

Remarque 2.0.0.1. La cohomologie galoisienne est un cas particulier de la cohomologie *étale* (voir exemple 1.1.1.3) : en effet, si K est un corps de groupe de Galois absolu G et de clôture séparable K_s, on a une équivalence de sites entre le site étale $(\mathrm{Spec}\, K)_{\mathrm{et}}$ et le site $G - \mathrm{Set}^{\mathrm{top}}$ des G-ensembles topologiques. Cette équivalence est donnée par :

$$X \mapsto X(K_s)$$

pour X un schéma étale au dessus de K, et dans l'autre sens, il suffit de le définir sur les G/U avec U sous-groupe ouvert de G, et on associe alors à G/U le schéma $\mathrm{Spec}(K_s^U)$. Les détails de cette équivalence sont dans [28], théorème 2.1.
Ainsi, tout G-module topologique A correspond à un faisceau abélien $\mathcal{A}$ sur le site $\mathrm{Spec}(K)_{\mathrm{et}}$ et on a :

$$H^n(K, A) = H^n_{\mathrm{et}}(\mathrm{Spec}(K), \mathcal{A}).$$

En ce sens, la cohomologie étale est une généralisation géométrique de la cohomologie galoisienne.

2.1 Hilbert 90

Le premier résultat fondamental de la cohomologie galoisienne est le suivant :

Théorème 2.1.0.1. *(Hilbert 90)*
Soit L/K une extension galoisienne. On a :

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

De façon plus générale, on a pour tout $m \geq 1$:

$$H^1(L/K, \mathrm{GL}_m(L)) = \{*\}.$$

Démonstration. Notons $G = \mathrm{Gal}(L/K)$. On choisit ici de donner une preuve qui peut sembler haut-perchée mais qui met en valeur la philosophie de la classification des formes tordues par le premier groupe de cohomologie, bien qu'il existe des preuves terre-à-terre en manipulant les cocycles.
En résumé, l'idée est que $H^1(L/K, \mathrm{GL}_m(L))$ classifie les formes tordues de L^m vu comme un faisceau via l'action canonique de G, or les espaces vectoriels sur K sont classifiés par leur dimension donc il n'y a qu'une seule forme tordue possible. Précisons cela : On utilise le théorème 1.1.6.6. Le site des G-ensembles topologiques est muni du faisceau d'anneaux $\mathcal{O} = h_L$ pour lequel :

$$\mathcal{O}(X) = \mathrm{Hom}_G(X, L)$$

pour tout G-ensemble topologique X.
Ainsi, $\mathrm{GL}_m(L)$ correspond au faisceau $\underline{\mathrm{Aut}}_{\mathcal{O}}(\mathcal{F})$ avec $\mathcal{F}$ le faisceau qui correspond à L^n.
Il faut donc montrer que si $\mathcal{F}'$ est un faisceau de $\mathcal{O}$-modules localement isomorphe à $\mathcal{F}$, alors il est isomorphe à $\mathcal{F}$.
Or un faisceau de $\mathcal{O}$-modules revient, par le lemme de Yoneda, à la donnée d'un L-espace vectoriel V muni d'une action de G compatible à la structure d'espace vectoriel. La théorie élémentaire de la descente galoisienne pour les espaces vectoriels assure alors que $V \cong V^G \otimes_K L$ et donc que V est simplement paramétré par sa dimension. Le fait que $\mathcal{F}'$ soit localement isomorphe à $\mathcal{F}$ entraîne que V est de dimension n, et donc il est isomorphe à $\mathcal{F}$. □

Le théorème suivant est parfois appelé théorème de Hilbert 90 additif. Il est évident en caractéristique nulle car $H^n(L/K, L)$ est alors à la fois un groupe de torsion et un K-espace vectoriel. La preuve en caractéristique quelconque est plus délicate.

Théorème 2.1.0.2. *(Hilbert 90 additif)*
Soit L/K une extension galoisienne. On a, pour tout $n \geq 1$:

$$H^n(L/K, L) = 0.$$

Démonstration. Par 1.2.1.8, on se ramène au cas où L/K est finie.
Notons $G = \mathrm{Gal}(L/K)$. Le théorème de la base normale affirme qu'il existe une K-base de L qui est une orbite sous l'action de G. Autrement dit, on a un isomorphisme de G-modules :

$$L \cong K[G] \cong \mathrm{Coind}_1^G K$$

ce qui donne le résultat voulu par le lemme de Shapiro 1.2.3.4. □

2.2 Théorie de Kummer

Soit K un corps et m un entier premier à la caractéristique de K. On note $G = \mathrm{Gal}(K_s/K)$ le groupe de Galois absolu de K. On dispose alors de la suite exacte de G-modules, appelée *suite de Kummer* :

$$1 \longrightarrow \mu_m \longrightarrow K_s^\times \xrightarrow{[m]} K_s^\times \longrightarrow 1$$

avec μ_m le groupe des racines m-èmes de l'unité dans K_s - il y en a bien m car $X^m - 1$ est séparable sur K - et $[m]$ la mise à la puissance m, que l'on verra plutôt comme la multiplication par m dans le groupe abélien $K_s^\times$. On obtient alors une suite exacte longue en cohomologie :

$$1 \longrightarrow \mu_m \cap K \longrightarrow K^\times \xrightarrow{[m]} K^\times \xrightarrow{\nabla} H^1(K, \mu_m) \longrightarrow 1$$

car $H^1(K, K_s^\times) = 0$ par Hilbert 90. On a ainsi un isomorphisme :

$$\nabla : \frac{K^\times}{(K^\times)^m} \cong H^1(K, \mu_m).$$

On peut expliciter l'isomorphisme puisqu'il est donné par le morphisme connectant ∇ : si $a \in K^\times$, on choisit un $a^{1/m} \in K_s^\times$ et on lui associe le cocycle suivant :

$$g \mapsto \varphi_a(g) = \frac{g a^{1/m}}{a^{1/m}} \in \mu_m.$$

Plaçons-nous à présent dans le *cas particulier où* $\mu_m \subseteq K$. Dans ce cas l'action de G sur μ_m est triviale et donc $H^1(G, \mu_m) = \mathrm{Hom}(G, \mu_m)$ est un sous-groupe du groupe des caractères de G (il est sous-entendu qu'on considère les morphismes *continus*). Expliquons comment ceci donne une preuve cohomologique de la classification des extensions cycliques.

Théorème 2.2.0.1. *Soit K un corps, K_s une clôture séparable de K et m un entier premier à la caractéristique de K tel que $\mu_m \subseteq K$. Notons E_m l'ensemble des extensions cycliques de K contenues dans K_s d'ordre divisant m et considérons le quotient de $K^\times/(K^\times)^m$ par l'action de $(\mathbb{Z}/m\mathbb{Z})^\times$ qui agit par exponentiation : $(k, a) \mapsto a^k$. On a alors une bijection :*

$$(K^\times/(K^\times)^m)/(\mathbb{Z}/m\mathbb{Z})^\times \cong E_m$$

via $a \mapsto K(a^{1/m})$. De plus, le groupe de Galois de $K(a^{1/m})/K$ est d'ordre d l'ordre de a dans le groupe $K^\times/(K^\times)^m$.

Démonstration. Notons S_m l'ensemble des sous-groupes normaux fermés de G dont le quotient est cyclique d'ordre divisant m qui est en bijection avec E_m par la théorie de Galois. On a les applications suivantes :

$$K^\times/(K^\times)^m \xrightarrow{\nabla} H^1(K, \mu_m) = \mathrm{Hom}(G, \mu_m) \xrightarrow{\mathrm{Ker}} S_m \xrightarrow{H \mapsto K_s^H} E_m$$

et seul Ker n'est pas nécessairement une bijection, mais elle est certainement surjective, et devient injective après quotient par l'action de $(\mathbb{Z}/m\mathbb{Z})^\times = \mathrm{Aut}(\mu_m)$, et pour voir cela on utilise le fait que si $d \mid m$ alors le morphisme $(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/d\mathbb{Z})^\times$ est surjectif.
Il est alors clair que a s'envoie sur $K(a^{1/m})$ vu la description du morphisme ∇ faite précedemment.
La correspondance des ordres est claire en inspectant la suite d'applications précédente. □

Notons qu'il est possible, étant donnée une extension cyclique L de degré m de K, avec $\mu_m \subseteq K$, de trouver un générateur a de L/K avec $a^m \in K$. Pour cela il sufit de considérer σ un générateur du groupe de Galois de L/K et de prendre un vecteur propre de σ pour une valeur propre racine primitive m-ème de l'unité. C'est ainsi qu'on prouve à la main le théorème précédent.

2.3 Théorie d'Artin-Schreier

La théorie d'Artin-Schreier permet de combler un cas non-traité par la théorie de Kummer : si K est de caractéristique p et que $m = p$. Son interprétation cohomologique se base sur la suite exacte suivante :

$$0 \longrightarrow \mathbb{F}_p \longrightarrow K_s \xrightarrow{\wp} K_s \longrightarrow 0$$

avec $\wp(x) = x^p - x$ qui est surjectif car pour tout $a \in K_s$, $X^p - X - a$ est un polynôme séparable.
Si $a \in K_s$, on notera abusivement $\wp^{-1}(a)$ pour un élément x tel que $x^p - x = a$, de sorte que $\wp^{-1}(a)$ n'est défini que modulo $\mathbb{F}_p$ (c'est un abus de notation équivalent à $a^{1/m}$ en théorie de Kummer). La suite exacte d'Artin-Schreier induit la suite exacte longue suivante en cohomologie :

$$0 \longrightarrow \mathbb{F}_p \longrightarrow K \xrightarrow{\wp} K \longrightarrow H^1(K, \mathbb{F}_p) \longrightarrow 0$$

car $H^1(K, K_s) = 0$. On a donc un isomorphisme :

$$\mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) = H^1(K, \mathbb{F}_p) \cong K/\wp K$$

car G agit trivialement sur $\mathbb{F}_p$. Par la même démonstration que 2.2.0.1, on en déduit le théorème suivant.

Théorème 2.3.0.1. *Soit K un corps de caractéristique $p > 0$, et K_s une clôture séparable de K. Notons E_p l'ensemble des extensions cycliques de K contenues dans K_s d'ordre p et considérons le quotient de $(K/\wp K) \setminus \{0\}$ par l'action de $(\mathbb{Z}/p\mathbb{Z})^\times$ qui agit par produit : $(k, a) \mapsto ka$. On a alors une bijection :*

$$((K/\wp K) \setminus \{0\}/(\mathbb{Z}/p\mathbb{Z})^\times)/ \cong E_p$$

via $a \mapsto k(\wp^{-1}a)$.

2.4 Algèbres centrales simples et groupe de Brauer d'un corps

Une des applications frappantes de la cohomologie galoisienne est la classification des algèbres centrales simples sur un corps par le second groupe de cohomologie du module galoisien associé au groupe multiplicatif. On commence par rappeler les définitions et premières propriétés des algèbres centrales simples sur un corps. Le but n'étant pas de faire un cours complet d'algèbre non-commutative, on renvoie à [20] pour les détails.

2.4.1 Premières propriétés des algèbres centrales simples

Un anneau *simple* est un anneau non-nul dont les seuls idéaux bilatères sont 0 et l'anneau tout entier. Ainsi, un corps est un anneau simple commutatif. Un *anneau à division* est un anneau non-nul dans lequel tout élément non-nul est inversible. Ainsi, tout anneau à division est simple et le centre d'un anneau simple est un corps.
L'analyse des idéaux bilatères de $M_n(A)$ montre que, pour $n \geq 1$, l'anneau $M_n(A)$ est simple si et seulement si l'anneau A est simple, et le centre de $M_n(A)$ est $A\,\mathrm{id}$.

Définition 2.4.1.1. *(Algèbre centrale simple sur un corps)*
Soit K un corps. Une algèbre centrale simple sur K est une K-algèbre simple de centre égal à K et de dimension finie sur K.

Le produit tensoriel de deux algèbres centrales simples est une algèbre centrale simple, et, si A est une algèbre centrale simple, alors $M_n(A)$ aussi. De plus, un théorème de Wedderburn assure que toute algèbre centrale simple sur K est isomorphe à $M_n(D)$ avec D une algèbre à division centrale (de dimension finie) sur K uniquement déterminée à isomorphisme près.
Si A est une algèbre centrale simple, on définit l'algèbre duale A^{opp} comme étant le même espace vectoriel sur K mais avec le produit suivant :

$$a *^{\mathrm{opp}} b = b * a.$$

On a alors un isomorphisme de K-algèbres :

$$A \otimes A^{\mathrm{opp}} \cong \mathrm{End}_K(A) \cong M_n(K)$$

avec n la dimension de A sur K. Cet isomorphisme est donné par $a \otimes a' \mapsto (x \mapsto axa')$.
L'idée de Brauer est alors d'identifier deux algèbres centrales simples sur K si elles sont de la forme $M_n(D)$ et $M_m(D)$ avec la même algèbre à division centrale sous-jacente D et de munir l'ensemble $\mathrm{Br}(K)$ des classes d'équivalence du produit tensoriel. Plus précisément, on définit l'équivalence à la Brauer de la façon suivante :

Définition 2.4.1.2. *Soient A et B deux algèbres centrales simples sur K. On dit qu'elles sont Brauer-équivalentes si elle sont isomorphes à des algèbres de matrices sur la même algèbre à division centrale. De façon équivalente, A et B sont Brauer-équivalentes s'il existe $p, q \geq 1$ vérifiant :*

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

On note $\mathrm{Br}(K)$ *l'ensemble des classes d'équivalence d'algèbres centrales simples sur K, qui forme bien un ensemble car ces algèbres peuvent êtres définies sur K^n avec n entier.*

On a toujours $M_n(A) \otimes M_m(B) \cong M_{mn}(A \otimes B)$ et donc $M_p(A) = A \otimes M_p(K)$. De façon équivalente, on peut définir $\mathrm{Br}(K)$ comme l'ensemble des classes d'isomorphisme d'algèbres à division centrales sur K.

Théorème 2.4.1.3. *(Groupe de Brauer)*
Soit K un corps. Le produit tensoriel des algèbres centrales simples est compatible à l'équivalence de Brauer et définit sur $\mathrm{Br}(K)$ *une structure de groupe commutatif dont l'élément neutre est K. L'inverse de $[A]$ est donné par $[A^{\mathrm{opp}}]$. On appelle ce groupe le groupe de Brauer de K.*

Démonstration. On a $M_m(D) \otimes M_n(D') \cong M_{mn}(D \otimes D')$ donc l'algèbre à division sous-jacente au produit tensoriel ne dépend que des algèbres à division sous-jacentes : il s'agit de prendre l'algèbre à division sous-jacente à $D \otimes D'$.
Ceci montre que la loi $\otimes$ descend sur l'ensemble $\mathrm{Br}(K)$. Elle est clairement commutative et associative et puisque $A \otimes A^{\mathrm{opp}}$ est une algèbre de matrices sur K, c'est l'élément neutre dans $\mathrm{Br}(K)$. □

Notons que deux algèbres centrales simples A et B sont isomorphes si et seulement si elles sont Brauer-équivalentes et de même dimension.

Exemple 2.4.1.4. Donnons deux exemples importants de groupes de Brauer.

- Si K est algébriquement clos, alors $\mathrm{Br}(K) = 0$. En effet, si D est une algèbre à division centrale (de dimension finie) sur K, alors pour tout $a \in D$, $K(a)$ est une extension finie de K donc $K(a) = K$ et ainsi $D = K$.
- Le groupe de Brauer de $\mathbb{R}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, et il est engendré par l'algèbre des quaternions $\mathbb{H}$.

2.4.2 Déploiement des algèbres centrales simples

Soit L/K une extension de corps. Si A est une K-algèbre centrale simple, alors $A_L = A \otimes_K L$ est une L-algèbre centrale simple. Cette considération fournit un morphisme de groupes, dit de restriction :

$$\mathrm{Br}(K) \xrightarrow{\mathrm{Res}_L^K} \mathrm{Br}(L)$$

dont on note $\mathrm{Br}(L/K)$ le noyau : c'est le groupe de Brauer relatif. On dit que *A se déploye sur L* si $[A]$ est dans le noyau de ce morphisme.
Puisque $\mathrm{Br}(\overline{K}) = 0$ avec K une clôture algébrique de K, on a $A_{\overline{K}}$ qui est isomorphe à une algèbre de matrices sur $\overline{K}$: en particulier la dimension de A sur K est un carré parfait. On pose alors :

$$\deg(A) = \sqrt{[A : K]}$$

le degré de A. On définit aussi l'indice de A comme le degré de l'algèbre à division sous-jacente à A : $\mathrm{ind}(A)$. Ainsi, l'indice de A ne dépend que de sa classe dans le groupe de Brauer de K. Le théorème suivant est fondamental et sa preuve repose sur le théorème de Skolem-Noether ainsi que le théorème du bicommutant. On renvoie à [20] pour une preuve.

Théorème 2.4.2.1. *(Caractérisation des corps de déploiement)*
Soit K un corps et A une algèbre centrale simple sur K. Soit L/K une extension finie. Alors L déploye A si et seulement s'il existe B une algèbre centrale simple sur K équivalente à A et un plongement de L dans B avec en plus :

$$\deg(B) = [L : K].$$

De plus, si $L \subseteq A$, on a toujours :

$$\deg_K(A) = [L : K] \deg_L(L')$$

avec $L' = C_A(L)$ le commutant de L dans A qui est une algèbre centrale simple sur L.

Notons que si L est un sous-corps d'une algèbre centrale simple A sur K, on a toujours :

$$[L : K] \mid \deg(A)$$

et donc cette condition sur le degré est une condition de maximalité du degré de L/K. Elle revient à dire que le commutant L' de L dans A est L.

Corollaire 2.4.2.2. *(Déploiement sur une extension finie séparable)*
Soit K un corps et A une algèbre centrale simple sur K. Il existe alors L/K une extension finie séparable qui déploye A. En particulier, si K est séparablement clos, alors $\mathrm{Br}(K) = 0$.

Démonstration. La preuve qu'on présente ici utilise un peu de géométrie algébrique.
On suppose K infini et de caractéristique $p > 0$, sinon il n'y a rien à prouver. En effet, on sait déjà que toute algèbre à division centrale D sur K se déploye sur $\overline{K}$, donc se déploye sur une extension finie de K car un isomorphisme $D_{\overline{K}} \cong M_n(\overline{K})$ descend sur une extension finie. Soit donc D une algèbre à division centrale de dimension finie sur K. Supposons que tout élément de $D \setminus K$ soit inséparable sur K. Il existe alors q une puissance de la caractéristique p du corps telle que $D^q \subseteq K$. On considère alors :

$$D \longrightarrow K$$

le morphisme de groupes $x \mapsto x^q$. Ce morphisme provient d'un morphisme de schémas $\varphi : \mathbb{A}^m_K \longrightarrow \mathbb{A}^1_K$ avec $m = \dim_K D$ car K est infini. On étend alors les scalaires à $\overline{K}$ pour obtenir au niveau des $\overline{K}$-points :

$$D_{\overline{K}} \longrightarrow \overline{K}$$

qui est toujours $x \mapsto x^q$, car c'est le cas sur les K-points et K est infini. Or $D_{\overline{K}}$ est une algèbre de matrices, et il existe des matrices qui à la puissance q ne donnent pas un multiple de l'identité, sauf si $D_{\overline{K}} = \overline{K}$.
On a donc montré que, si $D \neq K$, il existe un élément $a \in D \setminus K$ séparable sur K.
Ensuite, si L/K est une extension séparable avec $L \subseteq D$, on applique ce raisonnement à l'algèbre à division centrale sur L, $D' = C_D(L) \subseteq D$: si $D' \neq L$, il existe un élément de $D' \setminus L$ séparable sur L, ce qui donne une extension séparable L'/K contenue dans D strictement plus grosse. Au final, on aura $C_D(L) = L$ pour une certaine extension finie séparable L/K contenue dans D et donc L déploye A. □

2.4.3 Trace et norme réduite

Soit A une algèbre centrale simple sur un corps K. De la même façon que les extensions finies de K permettent de définir un polynôme homogène, la norme, il est possible de définir une norme *réduite* pour A. Un candidat naïf serait la norme d'algèbre $N_{A/K}$, mais on peut obtenir un polynôme de plus petit degré que ça par la construction suivante.
On a un isomorphisme de K_s-algèbres :

$$A_{K_s} \cong M_n(K_s).$$

En composant ce morphisme avec le déterminant et la trace, on obtient deux polynômes homogènes :

$$A_{K_s} \xrightarrow{\mathrm{N}} K_s^\times$$

et

$$A_{K_s} \xrightarrow{\mathrm{Tr}} K_s^\times.$$

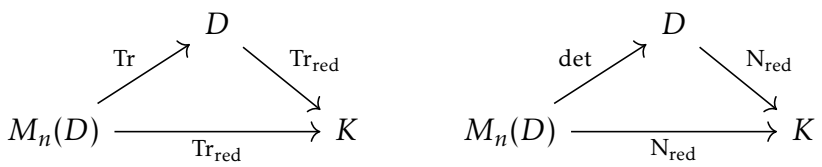
Ces polynômes sont invariants par l'action de Galois car si $\sigma \in G_K$, l'action de σ sur $M_n(K_s)$ et l'action de σ sur A_{K_s} déplacée par l'isomorphisme diffèrent d'un automorphisme intérieur de $M_n(K_s)$, et la trace et le déterminant sont invariants par ces automorphismes intérieurs. Ainsi, par descente galoisienne, on obtient une forme linéaire, dite de trace réduite :

$$A \xrightarrow{\mathrm{Tr}_{\mathrm{red}}} K$$

et un polynôme homogène de degré $n = \deg(A)$:

$$A \xrightarrow{\mathrm{N}_{\mathrm{red}}} K^\times.$$

Il est immédiat, à partir de la définition, que si $A = M_n(D)$, alors les diagrammes suivants commutent :



2.4.4 Interprétation cohomologique du groupe de Brauer

Soit K un corps de clôture séparable K_s. On explique ici comment le groupe de Brauer de K s'identifie au groupe $H^2(K, K_s^\times)$. Le fait que toute algèbre centrale simple sur K se déploye sur K_s (voir 2.4.2.2) permet de donner une définition alternative des algèbres centrales simples : ce sont exactement les K-algèbres A telles que A_{K_s} est isomorphe à une algèbre de matrices sur K_s. Autrement dit, ce sont des *formes tordues* de $M_n(K)$ sur le site $G_K - \mathrm{Set}^{\mathrm{top}}$ au sens de la philosophie générale présentée dans le théorème 1.1.6.5. Ici il faudrait adapter le théorème pour prendre en compte les automorphismes d'algèbres, néanmoins la preuve est exactement la même. On obtient ainsi la proposition suivante.

Proposition 2.4.4.1. *Soit K un corps et $m \geq 0$ un entier. On note $\mathrm{Br}^{(m)}(K)$ l'ensemble des classes d'isomorphisme d'algèbres centrales simples sur K de degré m. Puisque deux algèbres centrales simples A et B de même degré sont isomorphes si et seulement si elles sont Brauer-équivalentes, on a une inclusion : $\mathrm{Br}^{(m)}(K) \hookrightarrow \mathrm{Br}(K)$. On a alors un isomorphisme canonique :*

$$\mathrm{Br}^{(m)}(K) \cong H^1(K, \mathrm{PGL}_m(K_s)).$$

Démonstration. Par la philosophie générale des formes tordues, $\mathrm{Br}^{(m)}(K)$ s'identifie à $H^1(K, \mathrm{Aut}(M_n(K_s)))$ avec $\mathrm{Aut}(M_n(K_s))$ les automorphismes de K_s-algèbre de $M_n(K_s)$. Or le théorème de Skolem-Noether affirme que ces automorphismes sont tous intérieurs, d'où la conclusion. □

Notons ensuite que si $m \mid n$, on a un diagramme commutatif :

$$\begin{array}{ccc} \mathrm{Br}^{(m)}(K) & \xrightarrow{\bullet \otimes M_{n/m}(K)} & \mathrm{Br}^{(n)}(K) \\ \Big| & & \Big| \\ H^1(K, \mathrm{PGL}_m(K_s)) & \longrightarrow & H^1(K, \mathrm{PGL}_n(K_s)) \end{array}$$

où la flèche du bas provient du morphisme $\mathrm{PGL}_m(K_s) \longrightarrow \mathrm{PGL}_n(K_s)$ qui envoie une matrice M sur la matrice diagonale par blocs avec n/m blocs M. Ces morphismes de transition sont tous injectifs car si deux algèbres à division sont isomorphes après tensorisation par $M_{n/m}(K)$, elles sont équivalentes et, comme elles ont la même dimension, elles sont isomorphes. On a alors :

$$\mathrm{Br}(K) = \mathrm{colim}_m \mathrm{Br}^{(m)}(K) = \bigcup_m \mathrm{Br}^{(m)}(K).$$

via ces morphismes de transition pour $m \mid n$. On en déduit que :

$$\mathrm{Br}(K) = \mathrm{colim}_m H^1(K, \mathrm{PGL}_m(K_s)).$$

Observons alors la suite exacte suivante de G_K-groupes topologiques :

$$0 \longrightarrow K_s^\times \longrightarrow \mathrm{GL}_m(K_s) \longrightarrow \mathrm{PGL}_m(K_s) \longrightarrow 0.$$

Bien que les deux derniers groupes ne soient pas commutatifs, il est possible de démontrer avec la définition avec les cocycles, et parce que $K_s^\times$ s'envoie dans le centre de $\mathrm{GL}_m(K_s)$, qu'on a une suite exacte d'ensembles pointés, autrement dit l'image d'une flèche est l'ensemble des éléments qui s'envoient sur le point distingué par la flèche suivante de la suite :

$$H^1(K, K_s^\times) \longrightarrow H^1(K, \mathrm{GL}_m(K_s)) \longrightarrow H^1(K, \mathrm{PGL}_m(K_s)) \xrightarrow{\nabla} H^2(K, K_s^\times).$$

On a donc une application :

$$\mathrm{Br}^{(m)}(K) \longrightarrow H^2(K, K_s^\times)$$

qu'il est d'ailleurs possible d'expliciter via les cocycles. On renvoie alors au livre de Szamuely pour les détails de la preuve du théorème suivant.

Théorème 2.4.4.2. *(Groupe de Brauer et cohomologie)*
Soit K un corps. Les morphismes $\mathrm{Br}^{(m)}(K) \longrightarrow H^2(K, K_s^\times)$ sont compatibles et induisent un isomorphisme :

$$\mathrm{Br}(K) \cong H^2(K, K_s^\times)$$

en considérant $\mathrm{Br}(K)$ comme la colimite des $\mathrm{Br}^{(m)}(K)$.

En conséquence, le groupe de Brauer est un groupe de torsion : toute algèbre centrale simple sur K a un ordre dans le groupe de Brauer, appelé *période* de l'algèbre centrale simple, noté $\mathrm{per}(A)$. Si A est une algèbre centrale simple sur K, on a toujours l'indice qui divise la période :

$$\mathrm{ind}(A) \mid \mathrm{per}(A).$$

Avec l'identification donnée par le théorème, si L/K est une extension galoisienne, la suite exacte :

$$0 \longrightarrow \mathrm{Br}(L/K) \longrightarrow \mathrm{Br}(K) \longrightarrow \mathrm{Br}(L)$$

s'identifie à la suite d'inflation-restriction (voir 1.2.4.3) :

$$0 \longrightarrow H^2(L/K, L^\times) \xrightarrow{\mathrm{Inf}} H^2(K, K_s^\times) \xrightarrow{\mathrm{Res}} H^2(L, K_s^\times)$$

car $H^1(L, K_s^\times) = 0$. On a donc un isomorphisme canonique :

$$\mathrm{Br}(L/K) \cong H^2(L/K, L^\times).$$

Enfin, pour tout $m \geq 1$ non-nul dans le corps, la suite exacte de Kummer :

$$1 \longrightarrow \mu_m \longrightarrow K_s^\times \xrightarrow{[m]} K_s^\times \longrightarrow 1$$

donne en cohomologie, grâce à Hilbert 90 (2.1.0.1) :

$$H^2(K, \mu_m) \cong \mathrm{Ker}(\mathrm{Br}(K) \xrightarrow{[m]} \mathrm{Br}(K))$$

autrement dit :

$$H^2(K, \mu_m) = \mathrm{Br}(K)[m]$$

où la notation $[m]$ désigne la m-torsion.

2.4.5 Algèbres cycliques et algèbres de quaternions

Dans cette partie, on utilise l'interprétation cohomologique du groupe de Brauer pour étudier les algèbres cycliques sur un corps K, qui sont des exemples importans d'algèbres centrales simples sur K. On renvoie encore à [20] pour les détails.

Définition 2.4.5.1. *(Algèbre cyclique)*
Soit m un entier positif non-nul dans K, $\chi : G_K \longrightarrow \mathbb{Z}/m\mathbb{Z}$ un caractère continu surjectif du groupe de Galois et $b \in K^\times/(K^\times)^m$.
Le noyau G_L de χ est associé à une extension L/K de groupe de Galois $\mathbb{Z}/m\mathbb{Z}$, dont on note σ le générateur qui s'envoie sur 1 par χ. On définit une algèbre centrale simple (χ, b) comme la K-algèbre (non-commutative) générée par un élément β et par L telle que $\beta^m = b$ et $\lambda\beta = \beta\sigma(\lambda)$ pour tout $\lambda \in L$.

L'algèbre (χ, b) est de degré m et elle correspond au cocycle :

$$G_K \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathrm{PGL}_m(K)$$

qui envoie σ sur la matrice :

$$J = \begin{pmatrix} 0 & & & & b \\ 1 & & & & 0 \\ & 1 & & & 0 \\ & & \ddots & & \vdots \\ 0 & & & 1 & 0 \end{pmatrix}$$

car on a un isomorphisme :

$$\varphi : (\chi, b)_L \longrightarrow M_m(L)$$

qui envoie β sur J et $\lambda \in L$ sur la matrice diagonale de diagonale $(g(\lambda) \mid g \in \mathrm{Gal}(L/K))$, et donc l'automorphisme de $M_m(L)$ associé au fait de conjuguer φ par σ est donné par la conjugaison par J. On peut alors décrire la classe de (χ, b) dans le groupe $H^2(K, \mu_m) = \mathrm{Br}(K)[m]$.
Puisque $H^1(K, \mathbb{Z}/m\mathbb{Z})$ s'identifie au groupe des morphismes continus de G_K dans $\mathbb{Z}/m\mathbb{Z}$, on considère que $\chi \in H^1(K, \mathbb{Z}/m\mathbb{Z})$ et que $b \in H^1(K, \mu_m) = K^\times/(K^\times)^m$ (voir 2.2.0.1). On dispose alors du cup-produit :

$$H^1(K, \mathbb{Z}/m\mathbb{Z}) \otimes H^1(K, \mu_m) \longrightarrow H^2(K, \mu_m) = \mathrm{Br}(K)[m].$$

Proposition 2.4.5.2. *L'algèbre cyclique (χ, b) a pour classe $\chi \cup b$ dans le groupe* $\mathrm{Br}(K)[m]$.

L'idée de la preuve est de remonter χ à $H^0(K, \mathbb{Z})$ grâce à la suite exacte de G_K-modules triviaux $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$ et d'utiliser la compatibilité du cup-produit aux morphismes connectants. On réfère à [20] pour les détails du calcul.
Dans le cas où K possède les racines m-ème de l'unité, on peut donner une description plus élégante des algèbres cycliques. En effet, on a alors :

$$\mathbb{Z}/m\mathbb{Z} \cong \mu_m$$

comme G_K-modules via le choix d'une racine primitive m-ème ω. On peut donc choisir $a \in H^1(K, \mu_m) = K^\times/(K^\times)^m$ qui correspond à χ via cet isomorphisme, autrement dit $L = K(a^{1/m})$ et $\sigma(a^{1/m}) = \omega a^{1/m}$.
Dans ce cas, on adopte la notation suivante :

$$(a, b)_\omega = (\chi, b)$$

et on peut même décrire l'algèbre $(a, b)_\omega$ de la façon suivante : elle est engendrée par α et β qui vérifient $\alpha^m = a$ et $\beta^m = b$ et on a $\alpha\beta = \omega\beta\alpha$. La classe de $(a, b)_\omega$ dans le groupe de Brauer est alors donnée par $a \cup b \in H^2(K, \mu_m^{\otimes 2}) \cong \mathrm{Br}(K)[m]$ car $\mu_m \cong \mathbb{Z}/m\mathbb{Z}$ dans ce cas.

Définition 2.4.5.3. *(Algèbres de quaternions) Le cas $m = 2$ de la construction précédente donne les algèbres de quaternions sur K si K est de caractéristique différente de 2. On a donc une application bilinéaire :*

$$K^\times/(K^\times)^2 \otimes K^\times/(K^\times)^2 \longrightarrow \mathrm{Br}(K)[2]$$

qui envoie $a \otimes b$ sur $[(a, b)_{-1}] = a \cup b$. Par exemple, si $K = \mathbb{R}$, on retrouve l'algèbre de quaternions usuelle via la formule $(-1, -1)_{-1}$.

2.5 Dimension cohomologique des corps

La conjecture de Kato et Kuzumaki 6.0.0.1 propose de relier les propriétés diophantiennes des corps à leur dimension cohomologique, qui est l'invariant que nous allons étudier maintenant. On commence par le définir pour les groupes profinis car c'est là qu'il a tout son sens. Si A est un groupe abélien, on pose $A[p^\infty] = \bigcup_{r\geq 0} A[p^r]$ le sous-groupe des éléments annulés par une puissance de p.

Définition 2.5.0.1. *Soit G un groupe profini, p un nombre premier et $n \geq 0$ un entier. On dit que G est de p-dimension cohomologique au plus n, ce que l'on note :*

$$\mathrm{cd}_p(G) \leq n$$

si pour tout G-module discret de torsion A, et pour tout $i > n$, on a $H^i(G,A)[p^\infty] = 0$.
On définit alors la p-dimension cohomologique $\mathrm{cd}_p(G)$ de G comme le plus petit n tel que $\mathrm{cd}_p(G) \leq n$, et si un tel n n'existe pas, alors on pose $\mathrm{cd}_p(G) = \infty$.
Si k est un corps de caractéristique différente de p, on définit la p-dimension cohomologique de k, notée $\mathrm{cd}_p(k)$ comme la p-dimension cohomologique du groupe de Galois absolu de k.

On notera que les corps de p-dimension cohomologique 0 pour tout p sont les corps séparablement clos.

Remarque 2.5.0.2. Si A est un G-module discret de torsion, on peut écrire :

$$A = \bigoplus_p A[p^\infty]$$

et chaque $A[p^\infty]$ est un sous-G-module, de sorte que :

$$H^i(G,A)[p^\infty] = H^i(G, A[p^\infty]).$$

Par conséquent, on a $\mathrm{cd}_p(G) \leq n$ si et seulement si pour tout A G-module discret de p^∞-torsion et tout $i > n$, on a $H^i(G,A) = 0$.
Si $\mathrm{cd}_p(G) \leq n$ et si A est un G-module discret quelconque, en considérant les suites exactes $0 \longrightarrow A[p] \longrightarrow A \xrightarrow{p} pA \longrightarrow 0$ et $0 \longrightarrow pA \longrightarrow A \longrightarrow A/pA$, on obtient que $H^i(G,A)[p^\infty] = 0$ pour tout $i > n+1$.

Par un argument de décalage, il suffit de vérifier l'annulation de cohomologie pour $i = n+1$.

Proposition 2.5.0.3. *Si pour tout G-module discret de p^∞-torsion A, on a $H^{n+1}(G,A) = 0$, alors $\mathrm{cd}_p(G) \leq n$.*

Démonstration. On considère la suite exacte :

$$0 \longrightarrow A \longrightarrow \mathrm{Coind}_1^G A \longrightarrow C \longrightarrow 0$$

où tous les termes sont de p^∞-torsion. On a alors $H^i(G,A) = H^{i-1}(G,C)$, ce qui permet de conclure. □

Le résultat suivant permet de ramener le calcul de la dimension cohomologique à celui d'un p-Sylow qui est plus facile à établir.

Proposition 2.5.0.4. *Soit H un sous-groupe fermé de G. On a alors $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$, et si H est un pro-p-Sylow de G, il y a égalité.*
De plus, si G est un pro-p-groupe, on a $\mathrm{cd}_p(G) \leq n$ si et seulement si $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$, où $\mathbb{Z}/p\mathbb{Z}$ est muni de n'importe quelle action (on montre dans la preuve que cette action est nécessairement triviale).

Démonstration. Si A est un H-module discret de p^∞-torsion, on a $H^i(H, A) = H^i(G, \mathrm{Coind}_H^G A)$ et $\mathrm{Coind}_H^G(A)$ est encore de p^∞-torsion, d'où $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$.
Si maintenant H est un pro-p-Sylow de G, et si A est un G-module discret de p^∞-torsion, on a pour tout sous-groupe ouvert normal U de G le diagramme commutatif suivant :

$$H^i\left(G/U, A^U\right) \xrightarrow{\text{Res}} H^i\left(H/(U\cap H), A^U\right) \xrightarrow{\text{Cor}} H^i\left(G/U, A^U\right)$$
$$\overset{\curvearrowright}{\scriptstyle [G/U:H/(U\cap H)]}$$

avec $[G/U : H/(U \cap H)]$ qui est premier à p, et qui induit donc un isomorphisme puisque A est de p^∞-torsion. Ainsi res est injectif et cela permet de conclure : si $\mathrm{cd}_p(H) \leq n$, alors on montre que $H^i(G, A) = 0$ pour $i > n$ en considérant un $\alpha \in H^i(G, A)$, qui provient d'un certain $H^i(G/U, A^U)$ et dont la restriction à $H^i(H, A)$ est nulle par hypothèse, de sorte que, quitte à restreindre le sous-groupe ouvert normal U, on ait $\mathrm{res}(\alpha) = 0$ dans $H^i\left(H/(U \cap H), A^U\right)$ et donc $\alpha = 0$ par injectivité.
Supposons enfin que G est un pro-p-groupe. On veut voir que pour tout G-module discret A de p^∞-torsion, on a $H^{n+1}(G, A) = 0$. En écrivant A comme réunion croissante de sous-modules de type fini, on peut supposer A fini et annulé par p^r. Par un argument de dévissage très simple, on se ramène au cas où A est un G-module fini simple. Comme G est un pro-p-groupe, on a la formule :

$$\left|A^G\right| \equiv |A| \ [p]$$

et donc $A^G \neq 0$, et par simplicité $A^G = A$. On en déduit que $A = \mathbb{Z}/p\mathbb{Z}$ muni de l'action triviale. □

Remarque 2.5.0.5. La proposition précédente montre que la condition $\mathrm{cd}_p(k) \leq n$ pour un corps de caractéristique différente de p est stable par passage à une extension algébrique séparable. C'est aussi stable par passage à une extension algébrique quelconque car, si ℓ/k est une extension alébrique purement inséparable, et si $\overline{k}$ est une clôture algébrique de k et de ℓ, on a :

$$G_\ell = \mathrm{Hom}_\ell(\ell_s, \ell_s) = \mathrm{Hom}_\ell(\ell_s, \overline{k}) = \mathrm{Hom}_\ell(\overline{k}, \overline{k})$$

car $\overline{k}/\ell_s$ est purement inséparable, avec ℓ_s la clôture séparable de ℓ associée au choix de $\overline{k}$. De même, $G_k = \mathrm{Hom}_k(\overline{k}, \overline{k})$ et on remarque facilement qu'un morphisme φ de k-algèbres de $\overline{k}$ vers $\overline{k}$ est automatiquement ℓ-linéaire. En effet, si $x \in \overline{k}$ et $y \in \ell$, il existe r tel que $y^{q^r} \in k$ avec q la caractéristique de k, et on a :

$$\varphi(yx) = \left(\varphi(y^{q^r} x^{q^r})\right)^{q^{-r}} = y\varphi(x).$$

On a donc $G_k = G_\ell$, et la dimension cohomologique ne change pas (on vérifie bien sûr que les topologies sont les mêmes également).

Le théorème suivant concerne les corps de dimension au plus 1.

Théorème 2.5.0.6. *Soit k un corps et p un nombre premier. Si $\mathrm{car}(k) = p$, alors $\mathrm{cd}_p(G_k) \leq 1$.*
Sinon, les énoncés suivants sont équivalents :

1. $\mathrm{cd}_p(k) \leq 1$
2. *Pour toute extension algébrique séparable K/k, on a* $\mathrm{Br}(K)[p^\infty] = 0$.
3. *Pour toute extension algébrique séparable K/k, on a* $\mathrm{Br}(K)[p] = 0$.
4. *Pour toute extension algébrique séparable K/k et toute extension cyclique de degré p, L/K, la norme $L^\times \longrightarrow K^\times$ est surjective.*

Démonstration. Supposons d'abord que k est de caractéristique p. Dans ce cas, la suite exacte d'Artin-Schreier 2.3 donne :

$$H^2(G_k, \mathbb{Z}/p\mathbb{Z}) = 0.$$

En particulier, c'est aussi le cas pour $\ell = k_s^H$ avec H un pro-p-Sylow de G, et donc $\mathrm{cd}_p(G) = \mathrm{cd}_p(H) \leq 1$ d'après la proposition 2.5.0.4.
Supposons maintenant que $\mathrm{car}(k) \neq p$.
Puisque (1) est stable par passage aux extensions algébriques séparables, pour montrer (1) $\implies$ (2) il suffit de montrer que $\mathrm{Br}(k)[p^\infty] = 0$ en supposant $\mathrm{cd}_p(k) \leq 1$. Or on a :

$$\mathrm{Br}(k)[p^\infty] = \bigcup_{r \geq 0} H_2(G_k, \mu_{p^r}) = 0$$

par hypothèse. Ensuite, pour montrer (3) $\implies$ (4), on utilise le fait que pour une extension cyclique de degré p, on a :

$$K^\times / N(L^\times) = H^2(\mathrm{Gal}(L/K), L^\times) = \mathrm{Br}(L/K) \subseteq \mathrm{Br}(K)$$

et ce groupe est de p-torsion donc il est contenu dans $\mathrm{Br}(K)[p] = 0$.
Enfin, supposons (4) et montrons (1). On se ramène par la proposition 2.5.0.4 au cas où G_k est un pro-p-groupe et il suffit donc de montrer que $H^2(G_k, \mu_p) = 0$ par cette même proposition. Or :

$$H^2(G_k, \mu_p) = \mathrm{Br}(k)[p] = \bigcup_{\ell/k} \mathrm{Br}(\ell/k)[p]$$

où la réunion porte sur les ℓ/k galoisiennes finies. Puisqu'une telle extension est résoluble, on se ramène à montrer $\mathrm{Br}(\ell/k)[p] = 0$ pour ℓ/k cyclique de degré p, ce qui découle directement de l'observation $k^\times / N(\ell^\times) = \mathrm{Br}(\ell/k)$ faite précedemment. □

Le théorème précédent montre que l'invariant $\mathrm{cd}_p(G_k)$ n'a pas beaucoup d'intérêt quand k est de caractéristique p. On a donc recours à une définition différente dans ce cas (voir [14]), mais pour simplifier nous ne traiterons pas ces questions ici, de sorte que les preuves données ici fonctionnent en caractéristique nulle, mais il est toujours possible de généraliser à la caractéristique positive en prenant en compte cette définition alternative pour la p-dimension cohomologique.

Enfin, on définit aussi la dimension cohomologique *absolue* d'un corps k comme :

$$\mathrm{cd}(k) = \sup_p \mathrm{cd}_p(k).$$

2.6 Groupes de Tate-Chafarevitch

Un des ingrédients importants des preuves de cas particuliers de la conjecture de Kato et Kuzumaki pour des corps globaux est le passage du local au global. En d'autres termes, étant donné un

corps global K et un K-schéma X ayant des points dans tous les corps locaux associés à K, peut-on s'assurer que X possède un K-point ? Pour certains schémas, notamment les torseurs sous un groupe algébrique, la réponse est donnée par les groupes de Tate-Chafarevitch que nous allons définir à présent.
Soit K un corps global, c'est à dire un corps de nombres ou bien une extension finie du corps $k(t)$ avec k un corps fini. On note Ω_K l'ensemble de ses places et G_K le groupe de Galois de K.
Commençons par rappeler les faits suivants sur le caractère local-global de la théorie de Galois.

Proposition 2.6.0.1. *On note K_s une clôture séparable de K. Pour toute place v de K, il existe une place $\overline{v}$ de K_s au dessus de v et G_K agit transitivement sur l'ensemble des places au dessus de v. Notons $K^h_{s,\overline{v}}$ l'hensélisé de K_s en $\overline{v}$, c'est à dire la clôture séparable de K_v dans $K_{s,\overline{v}}$, qui s'identifie à $(K_v)_s$. Le stabilisateur $D(\overline{v},v)$ d'une place $\overline{v}$ au dessus de v est un sous-groupe fermé de G_K qui s'identifie comme groupe profini au groupe $\mathrm{Gal}(K^h_{s,\overline{v}}/K_v)$ qui est canoniquement isomorphe à G_{K_v}, le groupe de Galois absolu de K_v.*
Ainsi, quitte à choisir une place w de K_s au dessus de v, on a un plongement canonique de G_{K_v} dans G_K.
Enfin, si A est un G_K-module topologique, le morphisme de restriction $H^n(K,A) \xrightarrow{\mathrm{res}} H^n(K_v,A)$ ne dépend pas, à isomorphisme près, du choix de $\overline{v}$. Ainsi, on ne précisera pas le choix de $\overline{v}$ dans la suite.

Démonstration. Pour chaque extension finie L/K contenue dans K_s, notons $\Omega_{L,v}$ l'ensemble fini non-vide des places de L au dessus de v. La limite des $\Omega_{L,v}$ est non-vide comme limite projective d'ensembles finis non-vides, donc il existe une place $\overline{v}$ au dessus de v. De plus, si w_1, w_2 sont deux places au dessus de v, pour chaque L l'ensemble des $g \in \mathrm{Gal}(L/K)$ qui envoient $w_{1,|L}$ sur $w_{2,|L}$ est non-vide, et donc la limite de ces ensembles est encore non-vide. L'action est donc transitive.
Ensuite, si $\overline{v}$ est une place au dessus de v, le stabilisateur est donné par :

$$\bigcap_{L/K} \{g \in G_K \mid g^*_{|L}\overline{v}_{|L} = \overline{v}_{|L}\}$$

où l'intersection porte sur les extensions finies contenues dans K_s et ces groupes sont ouverts donc fermés. Ainsi le stabilisateur $D(\overline{v},v)$ est fermé. Tout élément de ce stabilisateur agit par isométries sur K_s muni de la place $\overline{v}$ et donc l'action s'étend de façon unique à la complétion $K_{s,\overline{v}}$ et se restreint ensuite à l'hensélisation. Réciproquement, tout élément de $\mathrm{Gal}(K^h_{s,\overline{v}}, K_v)$ agit sur K_s par $\overline{v}$-isométries et en fixant K, donc on a bien un isomorphisme canonique :

$$D(\overline{v},v) \cong \mathrm{Gal}(K^h_{s,\overline{v}}, K_v).$$

Ensuite, vérifions que $K^h_{s,\overline{v}}$ est une clôture séparable de K_v. On a déjà utilisé que l'extension est séparable, mais justifions le rapidement : pour toute extension finie intermédiaire L/K, on a :

$$L \otimes K_v = \prod_{w|v} L_w$$

de sorte que $0 = \Omega_{L/K} \otimes K_v = \Omega_{L\otimes K_v/K_v} = \bigoplus_{w|v} \Omega_{L_w/K_v}$.
De plus, par le lemme de Krasner et par densité de K dans K_v, toute extension finie séparable de K_v s'obtient comme corps de rupture d'un polynôme séparable à coefficients dans K irréductible sur K_v (et donc sur K), donc $K^h_{s,\overline{v}}$ est bien une clôture séparable de K_v.
La preuve du dernier énoncé vient du lemme général suivant. □

Lemme 2.6.0.2. *Soit G un groupe profini et H, K deux sous-groupes fermés conjugués de G. Pour tout G-module topologique A et tout entier $n \geq 0$, on a un triangle commutatif :*

$$\begin{array}{ccc} & H^n(G,A) & \\ {\scriptstyle \text{res}}\swarrow & & \searrow{\scriptstyle \text{res}} \\ H^n(K,A) & \xrightarrow{\sim} & H^n(H,A) \end{array}$$

où l'isomorphisme du bas est induit par le choix d'un σ dans G tel que $K = \sigma H \sigma^{-1}$.

Démonstration. Supposons que $K = \sigma H \sigma^{-1}$, de sorte que :

$$H^n(K,A) = H^n(H, A^\sigma)$$

avec A^σ le H-module dont l'action est donnée par $h * a = \sigma h \sigma^{-1} a$. On a alors un isomorphisme H-équivariant :

$$A^\sigma \longrightarrow A$$

donne par l'action de σ^{-1}. Ceci donne un isomorphisme $H^n(H, A^\sigma) \cong H^n(H, A)$ et permet de conclure. □

Définition 2.6.0.3. *(Groupes de Tate-Chafarevitch) Soit K un corps global et A un G_K-module topologique. On définit, pour tout $n \geq 0$, les groupes de Tate-Chafarevitch stricts :*

$$Ш^n(K,A) = \text{Ker}\left(H^n(K,A) \longrightarrow \prod_{v \in \Omega_K} H^n(K_v, A) \right)$$

et faible : $Ш^n_\omega(K,A)$ défini comme l'ensemble des $\alpha \in H^n(K,A)$ qui sont nuls dans presque tous les $H^n(K_v, A)$. Ces groupes sont bien définis et fonctoriels en A et en K grâce au lemme précédent. On a bien sûr :

$$Ш^n(K,A) \subseteq Ш^n_\omega(K,A) = 0.$$

Il est aussi possible de définir des groupes de Tate-Chafarevitch relatifs pour toute extension finie galoisienne L/K :

$$Ш^n(L/K,A) = \text{Ker}\left(H^n(L/K,A) \longrightarrow \prod_{v \in \Omega_K} H^n(L_{v'}/K_v, A) \right)$$

en choisissant des places v' de L au dessus de chaque v (encore une fois, le choix n'a pas d'importance). On définit de même le groupe de Tate-Chafarevitch relatif faible.

Il est possible de démontrer un lemme de Shapiro pour les groupes de Tate-Chafarevitch. Pour ce faire, commençons par rappeler l'énoncé suivant de théorie des représentations.

Proposition 2.6.0.4. *Soit G un groupe profini, H un sous-groupe ouvert de G et K un sous-groupe fermé de G. On considère $S \subseteq G$ une partie qui vérifie :*

$$G = \bigsqcup_{s \in S} HsK.$$

Soit A un H-module topologique. On a alors l'isomorphisme de K-modules topologiques suivant :

$$\text{Res}^G_K \text{Coind}^G_H A \cong \prod_{s \in S} \text{Coind}^K_{H \cap sKs^{-1}} A$$

où la coinduction de $H \cap sKs^{-1}$ à K se fait via le morphisme injectif $x \mapsto s^{-1}xs$.

Démonstration. Le cas où G est un groupe fini est bien connu, c'est par exemple un lemme qui permet d'obtenir le critère d'irréductibilité de Mackey. L'idée est que, dans ce cas, $\mathrm{Coind}_H^G A$ s'identifie à l'ensemble des applications $f : G \longrightarrow A$ qui sont H-équivariantes. À une telle application, on associe alors la famille de ses restrictions aux parties disjointes sK, que l'on précompose par la bijection $K \longrightarrow sK$ qui à k associe sk.
Puisque H est ouvert et G est compact, S est un ensemble *fini*.
On a, en faisant porter la colimite sur les sous-groupes ouverts distingués U de G contenus dans H (qui forment une base de voisinages de 1) et en notant $\pi_U : G \longrightarrow G/U$ la projection canonique :

$$\begin{aligned}
\mathrm{Coind}_H^G A &= \operatorname*{colim}_U \mathrm{Coind}_{H/U}^{G/U} A^U \\
&= \operatorname*{colim}_U \prod_{s\in S} \mathrm{Coind}_{\pi(H)\cap\pi(sKs^{-1})}^{\pi(K)} A^U \quad \text{car on a } G/U = \bigsqcup_{s\in S} (HsK)/U \text{ du fait que } U \subseteq H \\
&= \operatorname*{colim}_U \prod_{s\in S} \mathrm{Coind}_{\pi(H\cap sKs^{-1})}^{\pi(K)} A^U \quad \text{car } U \subseteq H \\
&= \prod_{s\in S} \operatorname*{colim}_U \mathrm{Coind}_{\pi(H\cap sKs^{-1})}^{\pi(K)} A^U \quad \text{car le produit est fini} \\
&= \prod_{s\in S} \mathrm{Coind}_{H\cap sKs^{-1}}^{K} A
\end{aligned}$$

comme voulu. On vérifie facilement que ces identifications sont K-équivariantes. □

Cette proposition nous permet de démontrer le lemme de Shapiro pour les groupes de Tate-Chafarevitch.

Théorème 2.6.0.5. *Soit K un corps global, $L \subseteq K_s$ une extension finie séparable de K et A un G_L-module topologique. On a des isomorphismes canoniques :*

$$Ш^n(K, \mathrm{Coind}_{G_L}^{G_K} A) \cong Ш^n(L, A)$$

et :

$$Ш^n_\omega(K, \mathrm{Coind}_{G_L}^{G_K} A) \cong Ш^n_\omega(L, A).$$

Démonstration. Soit v une place sur K, et fixons $\overline{v}$ une place sur K_s au dessus de v. Par la proposition 2.6.0.4 avec $G = G_K$, $H = G_L$ et $K = D(\overline{v} \mid v) = G_{K_v}$, on obtient :

$$\mathrm{Res}_{G_{K_v}}^{G_K} \mathrm{Coind}_{G_L}^{G_K} A \cong \prod_{s\in S} \mathrm{Coind}_{G_L\cap sD(\overline{v}|v)s^{-1}}^{D(\overline{v}|v)} A$$

avec S comme dans la proposition, c'est à dire que :

$$G_K = \bigsqcup_{s\in S} G_L s D(\overline{v} \mid v)$$

et avec la coinduction qui se fait via le morphisme de conjugaison par s.
Notons Λ l'ensemble des places de L au dessus de v. On a une application surjective (à cause de 2.6.0.1) :

$$G_K \longrightarrow \Lambda$$

qui à $\sigma \in G_K$ associe la place $((\sigma^{-1})^* \underline{v})_{|L}$. Cette application induit une bijection :

$$G_L \setminus G_K / D(\overline{v} \mid v) \cong \Lambda$$

ce qui permet de choisir le système de représentant S de sorte que S soit en bijection avec Λ via cette application.
Ainsi, si $s \in S$ correspond à w, on a $w = (s^{-1})^* \underline{v}$ et donc :

$$sD(\underline{v} \mid v)s^{-1} \cap G_L = D((s^{-1})^* \underline{v} \mid v) \cap G_L = D((s^{-1})^* \underline{v} \mid w).$$

Ceci permet de réécrire :

$$\mathrm{Res}^{G_K}_{G_{K_v}} \mathrm{Coind}^{G_K}_{G_L} A \cong \prod_{w \in \Lambda} \mathrm{Coind}^{D(\overline{v}|v)}_{D((s^{-1})^* \underline{v}|w)} A \cong \prod_{w \in \Lambda} \mathrm{Coind}^{G_{K_v}}_{G_{L_w}} A.$$

On a donc :

$$H^n(K_v, \mathrm{Coind}^{G_K}_{G_L} A) \cong \prod_{w \in \Lambda} H^n(L_w, A)$$

par le lemme de Shapiro habituel.
Ainsi :

$$\begin{aligned} Ш^n(K, \mathrm{Coind}^{G_K}_{G_L} A) &= \mathrm{Ker}\left(H^n\left(K, \mathrm{Coind}^{G_K}_{G_L} A\right) \longrightarrow \prod_v H^n\left(K_v, \mathrm{Coind}^{G_K}_{G_L} A\right)\right) \\ &= \mathrm{Ker}\left(H^n(L, A) \longrightarrow \prod_v \prod_{w|v} H^n(L_w, A)\right) = Ш^n(L, A). \end{aligned}$$

En adaptant ce dernier argument, on obtient également la preuve pour les groupes $Ш^n_\omega$. □

Corollaire 2.6.0.6. *Soit K un corps global et X un ensemble fini sur lequel G_K agit. On note A le module de permutation associé, c'est à dire $A = \mathbb{Z}[X]$ muni de l'action évidente de G_K. Alors on a :*

$$Ш^2(K, A) = Ш^2_\omega(K, A) = 0.$$

Démonstration. Les foncteurs $Ш^n$ et $Ш^n_\omega$ étant additifs, on peut supposer que X est un G_K-ensemble transitif quitte à décomposer X en union disjointe d'orbites. Ainsi, on peut identifier X à un quotient fini G_K/G_L par la correspondance de Galois, avec L/K une extension finie séparable de K contenue dans K_s. Par le lemme de Shapiro pour les groupes de Tate-Chafarevitch 2.6.0.5, on a donc :

$$Ш^2_\omega(K, A) = Ш^2_\omega(K, \mathrm{Coind}^{G_K}_{G_L} \mathbb{Z}) = Ш^2_\omega(L, \mathbb{Z})$$

et on peut donc supposer que $A = \mathbb{Z}$, muni de l'action triviale.
On utilise alors la suite exacte suivante :

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Rappelons que le module galoisien trivial $\mathbb{Q}$ n'a pas de cohomologie, de sorte que :

$$Ш^2_\omega(K, \mathbb{Z}) = Ш^1_\omega(K, \mathbb{Q}/\mathbb{Z})$$

par la compatibilité de la suite exacte longue en cohomologie aux morphismes de restrictions. Le groupe $H^1(K, \mathbb{Q}/Z)$ est le groupe des caractères continus de G_K, et si un caractère continu de G_K est nul sur chaque G_{K_v} pour presque toute place v de K, alors il est nul à cause du théorème de densité de Chebotarev : en effet, par continuité un tel caractère se factorise par un groupe de Galois fini $\mathrm{Gal}(L/K)$, et le théorème de Chebotarev, valable aussi pour les corps de fonctions, assure que tout élément de ce groupe provient d'une infinité de places finies non ramifiées. On a donc $Ш^1_\omega(K, \mathbb{Q}/\mathbb{Z}) = 0$ d'où la conclusion. □

Chapitre 3

Groupes algébriques

3.1 Généralités

Soit k un corps. Un groupe algébrique sur k est un schéma en groupes Γ de type fini sur k. Autrement dit, c'est un schéma de type fini sur k muni d'une factorisation (à isomorphisme naturel près) du foncteur des points par la catégorie des groupes :

$$\mathrm{Sch}_k \longrightarrow \mathrm{Grp} \longrightarrow \mathrm{Set}$$

ce qui revient à dire que pour tout k-schéma X, $\Gamma(X)$ est un groupe et pour chaque morphisme $X \longrightarrow Y$ de k-schémas, la flèche $\Gamma(Y) \longrightarrow \Gamma(X)$ est un morphisme de groupes.
Il est facile de voir que ça revient à munir chaque $\Gamma(R)$ d'une structure de groupe pour toute k-algèbre R de sorte que si $R \longrightarrow S$ est un morphisme de k-algèbres, alors $\Gamma(R) \longrightarrow \Gamma(S)$ est un morphisme de groupes.
De façon équivalente, une structure de groupe algébrique sur Γ peut être donnée par des morphismes $\Gamma \times_k \Gamma \longrightarrow \Gamma$ (multiplication), $\Gamma \longrightarrow \Gamma$ (inversion) et $\mathrm{Spec}(k) \longrightarrow \Gamma$ (unité) qui vérifient les axiomes de groupe, ou, ce qui est équivalent, par Yoneda, tels que pour tout R une k-algèbre, les applications induites $\Gamma(R) \times \Gamma(R) \longrightarrow \Gamma(R)$, $\Gamma(R) \longrightarrow \Gamma(R)$ et $\{\bullet\} \longrightarrow \Gamma(R)$ fassent de $\Gamma(R)$ un groupe.

Si Γ est affine, tout ceci est encore équivalent à la donnée d'une structure d'*Algèbre de Hopf* sur $A = \mathcal{O}(\Gamma)$, c'est à dire d'un morphisme de comultiplication $\Delta : A \longrightarrow A \otimes_k A$, d'un morphisme antipode $A \longrightarrow A$ et d'une counité $\varepsilon : A \longrightarrow k$ qui vérifient les axiomes duaux.

Exemple 3.1.0.1. On introduit les notations suivantes : le groupe multiplicatif $\mathbb{G}_m$ ou $(\mathbb{G}_m)_k$ défini comme $\mathrm{Spec}\, k[T, 1/T]$ et le groupe additif $\mathbb{G}_a$ ou $(\mathbb{G}_a)_k$ défini comme $\mathrm{Spec}\, k[T]$.

Si $f : \Gamma \longrightarrow \Gamma'$ est un morphisme de groupes algébriques sur k, on définit le noyau de f, $\mathrm{Ker}(f)$, comme le tiré en arrière de l'unité $\mathrm{Spec}(k) \longrightarrow \Gamma'$ par f. Il est immédiat de vérifier que c'est un sous-groupe fermé de Γ, et qu'on a pour tout R une k-algèbre :

$$\mathrm{Ker}(f)(R) = \mathrm{Ker}(\Gamma(R) \longrightarrow \Gamma'(R)).$$

Rappelons ensuite le théorème de Cartier ainsi que les propriétés géométriques de base des groupes algébriques.

Théorème 3.1.0.2. *Soit Γ un groupe algébrique sur un corps k. Alors Γ est séparé et son faisceau cotangent est trivial. Si k est de caractéristique nulle, alors Γ est lisse.*

En particulier, un groupe algébrique en caractéristique 0 est réduit et ses composantes connexes sont ses composantes irréductibles.

Démonstration. Soit Γ un groupe algébrique sur k. On commence par montrer que le faisceau cotangent est trivial : plus précisément, si $e : \mathrm{Spec}(k) \longrightarrow \Gamma$ est le morphisme unité et si $f : \Gamma \longrightarrow \mathrm{Spec}(k)$ est le morphisme structural, alors on a :

$$\Omega_{\Gamma/k} = f^* e^* \Omega_{\Gamma/k}$$

et comme $e^*\Omega_{\Gamma/k}$ est libre de dimension $\dim_k T_e^*\Gamma$, c'est aussi le cas du tiré en arrière par f. Pour cela, on note $\mu : \Gamma \times_k \Gamma \longrightarrow \Gamma$ la multiplication et $p_1, p_2 : \Gamma \times_k \Gamma \longrightarrow \Gamma$ les deux projections. On note aussi $\sigma : \Gamma \times_k \Gamma \longrightarrow \Gamma \times_k \Gamma$ le morphisme qui, sur les points, est donné par $(x, y) \mapsto (xy, y)$. C'est un isomorphisme de schémas au dessus de Γ via la projection p_2, et ainsi on a :

$$\sigma^* \Omega_{\Gamma \times_k \Gamma/\Gamma} \cong \Omega_{\Gamma \times_k \Gamma/\Gamma}$$

et d'autre part $\Omega_{\Gamma \times_k \Gamma/\Gamma} = p_1^* \Omega_{\Gamma/k}$. On tire en arrière par $\varphi : \Gamma \longrightarrow \Gamma \times_k \Gamma$ qui, sur les points, est donné par $g \mapsto (e, g)$, ce qui donne :

$$\Omega_{\Gamma/k} = (p_1 \circ \sigma \circ \varphi)^* \Omega_{\Gamma/k} = \varphi^* \sigma^* \Omega_{\Gamma \times_k \Gamma/\Gamma} \cong \varphi^* \Omega_{\Gamma \times_k \Gamma/\Gamma} = (p_1 \circ \varphi)^* \Omega_{\Gamma/k} = f^* e^* \Omega_{\Gamma/k}.$$

Si k est de caractéristique 0, comme Γ est de type fini sur k, la locale liberté du faisceau tangent entraîne que Γ est lisse. Γ est séparé (sur k) car on a le diagramme commutatif cartésien suivant :

$$\begin{array}{ccc} \Gamma & \xrightarrow{\Delta} & \Gamma \times_k \Gamma \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle (x,y)\mapsto x^{-1}y} \\ \mathrm{Spec}(k) & \xrightarrow[e]{} & \Gamma \end{array}$$

et e est clairement une immersion fermée car Γ est un k-schéma de type fini.

□

Proposition 3.1.0.3. *Soit Γ est un groupe algébrique réduit sur k. Γ est le groupe trivial si et seulement si $\Gamma(\Omega)$ est le groupe trivial pour Ω un corps algébriquement clos contenant k.*

Démonstration. Si $\Gamma(\Omega)$ est trivial, alors pour tout point fermé x de Γ, le corps résiduel $k(x)$ est une extension finie de k car Γ est de type fini sur k et donc $k(x)$ se plonge dans Ω, ce qui donne un morphisme :

$$\mathrm{Spec}(\Omega) \longrightarrow \mathrm{Spec}\, k(x) \longrightarrow \Gamma$$

et par hypothèse, il n'y en a qu'un. On en déduit que Γ n'a qu'un seul point fermé et donc que Γ est le groupe trivial. □

3.2 Groupes algébriques affines

Dans la suite, on sera intéressé seulement par des groupes algébriques affines sur un corps k. Si $f : \Gamma \longrightarrow \Gamma'$ est un morphisme de groupes algébriques affines sur k, les bonnes notions d'injectivité et de surjectivité de f sont données respectivement par le fait que f soit une immersion fermée et le fait que f soit fidèlement plat (on dit alors que f est un quotient). Dans notre cas, ces propriétés peuvent se vérifier de façon plus élémentaire, comme on va le voir.
La preuve du théorème suivant repose sur des énoncés techniques sur les algèbres de Hopf, notamment le fait que toute inclusion d'algèbres de Hopf de type fini sur k est fidèlement plate. On renvoie à [18] pour une preuve.

Théorème 3.2.0.1. *Tout morphisme de groupes algébriques affines sur k, $f : \Gamma \longrightarrow \Gamma'$, se factorise en $\Gamma \longrightarrow \mathrm{Im}(f) \longrightarrow \Gamma'$ avec $\mathrm{Im}(f)$ un certain sous-groupe fermé uniquement déterminé de Γ' et $\Gamma \longrightarrow \mathrm{Im}(f)$ un quotient.*

Corollaire 3.2.0.2. *Si $f : \Gamma \longrightarrow \Gamma'$ est un quotient de groupes algébriques affines sur k et $\mathrm{Ker}(f)$ est le groupe trivial, alors f est un isomorphisme.*

Démonstration. Par Yoneda, il suffit de montrer que pour tout R une k-algèbre, on a un isomorphisme $\Gamma(R) \longrightarrow \Gamma'(R)$. Par hypothèse, ce morphisme est injectif. Soit ensuite $y \in \Gamma'(R)$. Par fidèle platitude de Γ sur Γ', il existe S une R-algèbre fidèlement plate et $x \in \Gamma(S)$ tel que x s'envoie sur y vu dans $\Gamma'(S)$: en effet, il suffit de prendre $S = R \otimes_{\mathcal{O}(\Gamma')} \mathcal{O}(\Gamma)$ qui est fidèlement plat comme changement de base du morphisme fidèlement plat $\mathcal{O}(\Gamma') \longrightarrow \mathcal{O}(\Gamma)$. On montre ensuite que :

$$R = \lim (S \rightrightarrows S \otimes_R S)$$

autrement dit, comme $R \subseteq S$, que $R = \{s \in S \mid s \otimes 1 = 1 \otimes s\}$. En effet, si $s \otimes 1 = 1 \otimes s$, on a $1 \otimes s \in S \otimes R \subseteq S \otimes S$ car S/R est plat, et donc l'image de $1 \otimes s$ dans le quotient $(S \otimes S)/(S \otimes R) = S \otimes (S/R)$ est nulle. Si on note L le R-module engendré par l'image de s dans S/R, on a donc $S \otimes_R L = 0$ et par fidèle platitude, on en déduit que $L = 0$ et donc que $s \in R$ comme souhaité. On a donc :

$$\Gamma(R) = \lim (\Gamma(S) \rightrightarrows \Gamma(S \otimes S))$$

et

$$\Gamma'(R) = \lim (\Gamma'(S) \rightrightarrows \Gamma'(S \otimes S))$$

ce qui est tout l'intérêt de la descente fidèlement plate. Il est alors facile de voir que $x \in \Gamma(S)$ vit dans cette limite en utilisant l'injectivité des $\Gamma(T) \longrightarrow \Gamma'(T)$ et donc que $x \in \Gamma(R)$, ce qui permet de conclure. □

Corollaire 3.2.0.3. *Soit $f : \Gamma \longrightarrow \Gamma'$ un morphisme de groupes algébriques affines réduits sur k et soit Ω un corps algébriquement clos contenant k. On a alors d'une part les équivalences suivantes :*

- *f est une immersion fermée.*
- *$\mathrm{Ker}(f)$ est le groupe algébrique trivial.*
- *f est injective au niveau des Ω-points et $\mathrm{Ker}(f)$ est réduit (cette deuxième condition est immédiate en caractéristique nulle).*

et d'autre part les équivalences suivantes :

- *f est un quotient.*
- *$\mathrm{Im}(f) = \Gamma'$ comme sous-schémas fermés de Γ'.*
- *f est dominante.*
- *f est surjective au niveau des Ω-points.*

Démonstration. Si f est une immersion fermée, c'est un monomorphisme et donc son noyau est trivial par le lemme de Yoneda. Les points 2 et 3 sont équivalents à cause de la proposition 3.1.0.3. Enfin, si $\mathrm{Ker}(f)$ est le groupe trivial, on factorise f en :

$$\Gamma \xrightarrow{q} \mathrm{Im}(f) \xrightarrow{i} \Gamma'$$

avec i une immersion fermée et q un quotient. Ainsi, q est encore un monomorphisme et par le corollaire 3.2.0.2, c'est un isomorphisme. On en déduit que f est une immersion fermée.
Si f est un quotient, l'espace topologique sous-jacent à $\mathrm{Im}(f)$ est Γ' car f est surjective sur les points, et c'est aussi une égalité schématique car $\mathrm{Im}(f)$ est réduit, puisque $\mathcal{O}(\mathrm{Im}(f)) \hookrightarrow \mathcal{O}(\Gamma)$. Si $\mathrm{Im}(f) = \Gamma'$, alors f est clairement surjective sur les points et donc dominante. Ensuite, si f est dominante, $\mathrm{Im}(f)$ contient une partie dense donc $\mathrm{Im}(f) = \Gamma$ (encore une fois parce qu'il est réduit) et donc i est un isomorphisme et f est un quotient.
Il reste à voir l'équivalence avec le dernier point. Si f est un quotient, alors pour tout $y \in \Gamma'(\Omega)$, par le même argument que dans la preuve de 3.2.0.2, on trouve $x \in \Gamma(S)$ qui s'envoie sur y avec S une Ω-algèbre fidèlement plate. Puisque $\mathcal{O}(\Gamma)$ est de type fini sur k, le morphisme $\mathcal{O}(\Gamma) \longrightarrow S$ associé à x est à valeurs dans une sous-Ω-algèbre de type fini non-nulle (car S est fidèlement plate), et donc on peut supposer S non-nulle et de type fini. Par le Nulstellensatz, elle possède un Ω-point, ce qui donne bien un Ω-point de Γ qui s'envoie sur y par une vérification élémentaire.
Supposons enfin que f est surjective au niveau des Ω-points. Elle est alors dominante à cause du diagramme commutatif suivant (ou $|\Gamma|$ est l'espace topologique sous-jacent à Γ) :

$$\begin{array}{ccc} \Gamma(\Omega) & \twoheadrightarrow & \Gamma'(\Omega) \\ \downarrow & & \downarrow \\ |\Gamma| & \longrightarrow & |\Gamma'| \end{array}$$

en observant que les flèches verticales sont d'image dense (leurs images contiennent les points fermés). □

On peut maintenant définir ce qu'est une suite exacte de groupes algébriques affines sur k.

Définition 3.2.0.4. *Une suite de morphismes de groupes algébriques affines sur k, $\Gamma_1 \xrightarrow{f} \Gamma_2 \xrightarrow{g} \Gamma_3$ est exacte si $g \circ f$ est le morphisme trivial et le morphisme induit $\Gamma_1 \longrightarrow \mathrm{Ker}(g)$ est un quotient.*

Proposition 3.2.0.5. *Soit k un corps de caractéristique nulle, Ω un corps algébriquement clos contenant k et $\Gamma_1 \xrightarrow{f} \Gamma_2 \xrightarrow{g} \Gamma_3$ une suite de groupes algébriques affines sur k. Cette suite est exacte si et seulement si la suite induite sur les Ω-points est exacte (au sens usuel de la théorie des groupes abstraits).*

Démonstration. On est en caractéristique nulle donc les problèmes de nilpotence ne se posent pas.
Si $\Gamma_1 \xrightarrow{f} \Gamma_2 \xrightarrow{g} \Gamma_3$ est exacte, on a bien $g \circ f = 1$ au niveau des Ω-points par fonctorialité, et le morphisme induit $\Gamma_1 \longrightarrow \mathrm{Ker}(g)$ étant un quotient, il est surjectif sur les Ω-points, or $\mathrm{Ker}(g)(\Omega) = \mathrm{Ker}(\mathrm{g}(\Omega))$, donc $\Gamma_1(\Omega) \longrightarrow \mathrm{Ker}(\Gamma_2(\Omega) \longrightarrow \Gamma_3(\Omega))$ est surjectif.
Si $\Gamma_1(\Omega) \longrightarrow \Gamma_2(\Omega) \longrightarrow \Gamma_3(\Omega)$ est une suite exacte de groupes abstraits, on a $\mathrm{Ker}(g \circ f) \hookrightarrow \Gamma_1$ qui est une immersion fermée et un quotient car elle est surjective au niveau des Ω-points, donc c'est un isomorphisme et $g \circ f$ est le morphisme trivial. Le morphisme induit $\Gamma_1 \longrightarrow \mathrm{Ker}(g)$ est un quotient car il est surjectif sur les Ω-points. □

3.3 Groupes de type multiplicatif en caractéristique nulle

On présente dans cette partie la théorie des groupes de type multiplicatif sur un corps k, qu'on prend de caractéristique nulle pour plus de simplicité, bien que la théorie s'adapte aussi en caracté-

ristique positive. Les groupes de type multiplicatif rassemblent les tores et les groupes abéliens finis en une catégorie MT_k, duale de la catégorie des G_k-modules topologiques de type fini sur $\mathbb{Z}$.
Soit k un corps de caractéristique nulle et $\overline{k}$ une clôture algébrique. On rappelle qu'un tore sur k désigne un groupe algébrique affine sur k qui, après changement de base à $\overline{k}$, est isomorphe à $\mathbb{G}_m^d$. On dit que le tore T est diagonalisable sur k s'il est isomorphe à $\mathbb{G}_m^d$ sur k.
D'autre part, les groupes finis sur k sont les groupes algébriques affines finis sur k, ou, de façon équivalente, qui ont un nombre fini de points dans $\overline{k}$.
Si F est un groupe fini abstrait, on lui associe le groupe fini sur k, $\underline{F} = \bigsqcup_{f\in F} \mathrm{Spec}(k)$. C'est bien un groupe algébrique car pour toute k-algèbre R, on a $\underline{F}(R)$ qui est en bijection naturelle avec l'ensemble des fonctions localement constantes de $\mathrm{Spec}\, R$ dans F.
On s'intéresse ensuite à la notion de groupe de type multiplicatif, qui rassemble les tores et les groupes abéliens finis sur k.

Définition 3.3.0.1. *Un groupe de type multiplicatif sur k est un groupe algébrique affine Γ sur k isomorphe au produit d'un tore et d'un groupe fini abélien sur k. On dit qu'un groupe de type multiplicatif est diagonalisable sur k s'il est isomorphe à $\mathbb{G}_m^d \times_k \underline{F}$ avec F un groupe abélien fini.*

On note MT_k la catégorie des groupes de type multiplicatif sur k. Si Γ est un groupe algébrique commutatif sur k, on définit le groupe des caractères et le groupe des cocaractères respectivement comme :

$$X^*(\Gamma) = \mathrm{Hom}(\Gamma_{\overline{k}}, \mathbb{G}_m) \subseteq \mathrm{Hom}(\Gamma(\overline{k}), \overline{k}^\times)$$

et

$$X_*(\Gamma) = \mathrm{Hom}(\mathbb{G}_m, \Gamma_{\overline{k}})$$

où l'on considère à chaque fois les morphismes de groupes algébriques sur $\overline{k}$. On voit notamment que ces définitions ne changent pas si l'on fait un changement de base algébrique.
Le groupe de Galois absolu de k, G_k, agit à gauche sur $\Gamma_{\overline{k}}$ par automorphismes de k-schémas (via l'action à droite sur A donnée par $f \mapsto f^{\sigma^{-1}}$) et donc il agit à gauche sur $X^*(\Gamma)$ de la façon suivante : si $\sigma \in G_k$ et $\chi \in X^*(\Gamma)$, on définit $\sigma \cdot \chi$ ainsi :

$$\Gamma_{\overline{k}} \xrightarrow{\sigma^{-1}} \Gamma_{\overline{k}} \longrightarrow \mathbb{G}_m \xrightarrow{\sigma} \mathbb{G}_m$$

de sorte que les points fixes de l'action correspondent aux morphismes $\Gamma \longrightarrow \mathbb{G}_m$. De même, G_k agit à gauche sur le groupe des cocaractères.
Voyons tout de suite des exemples.

Lemme 3.3.0.2. *On a $X^*(\mathbb{G}_m) = X_*(\mathbb{G}_m) = \mathbb{Z}$ muni de l'action triviale de G_k et si F est un groupe fini commutatif, $X^*(\underline{F}) = F^\vee$ et $X_*(\underline{F}) = F$, avec $F^\vee$ le groupe des caractères de F, et toujours avec l'action triviale de G_k.*

Démonstration. Pour le premier cas, il s'agit de déterminer les endomorphismes d'anneau de $\overline{k}[T, 1/T]$ qui induisent un endomorphisme de groupes algébriques. Un tel morphisme est déterminé par un élément inversible de $k[T, 1/T]$, c'est à dire un élément de la forme αT^n avec $\alpha = 1$ pour qu'on ait bien un morphisme d'algèbres de Hopf, et $n \in \mathbb{Z}$. Ainsi les caractères sont en bijection avec $\mathbb{Z}$, avec χ_n le caractère $x \mapsto x^n$. L'action de Galois est triviale car tous ces morphismes sont définis sur k.
Ensuite, on a :

$$X^*(\underline{F}) = \mathrm{Hom}_{\text{gp-alg}}\left(\bigsqcup_{f\in F} \mathrm{Spec}(\overline{k}), \mathbb{G}_m\right) = \mathrm{Hom}(F, \overline{k}^\times) = F^\vee$$

car k est de caractéristique nulle. Ensuite, $X_*(\underline{F})$ est contenu dans $\underline{F}(\mathbb{G}_m)$, l'ensemble des fonctions localement constantes de $\mathbb{G}_m$ dans F, or $\mathbb{G}_m$ est connexe donc c'est isomorphe à F. □

On se convainc facilement que si Γ et Γ' sont deux groupes algébriques affines commutatifs sur k, on a $X^*(\Gamma \times_k \Gamma') = X^*(\Gamma) \times X^*(\Gamma')$ et $X_*(\Gamma \times_k \Gamma') = X_*(\Gamma) \times X_*(\Gamma')$ de façon compatible à l'action de Galois. Ceci assure que $X^*(\Gamma)$ est toujours de type fini sur $\mathbb{Z}$ pour Γ de type multiplicatif, et l'action de Galois est toujours continue car, en étendant les scalaires sur une extension finie où le groupe Γ est diagonalisable, l'action devient triviale.
Ainsi, en notant $G_k - \mathrm{Mod}^f$ la catégorie des G_k-modules continus de type fini sur $\mathbb{Z}$, on a un foncteur :

$$(\mathrm{MT}_k)^{\mathrm{op}} \longrightarrow G_k - \mathrm{Mod}^f$$

qui à Γ associe son groupe de caractères. On va montrer que c'est une *équivalence de catégories*.
Commençons par observer que, par le principe d'indépendance des caractères, $X^*(\Gamma)$ est toujours une famille $\overline{k}$-libre de la $\overline{k}$-algèbre $A = \mathcal{O}(\Gamma_{\overline{k}})$. On peut caractériser le fait que Γ soit de type multiplicatif par le fait que cette famille soit une base.

Proposition 3.3.0.3. *Soit Γ un groupe algébrique affine sur k de caractéristique 0. Les énoncés suivants sont équivalents :*

- *Γ est de type multiplicatif.*
- *$X^*(\Gamma)$ est une $\overline{k}$-base de $A = \mathcal{O}(\Gamma_{\overline{k}})$.*
- *$\Gamma_{\overline{k}}$ est isomorphe à un sous-groupe fermé d'un tore*

Démonstration. On peut supposer k algébriquement clos.
Pour montrer $1 \implies 2$, il suffit d'observer que 2 est valable pour les tores et les groupes abéliens finis, ce qu'on vient de démontrer.
Supposons à présent que $X^*(\Gamma)$ est une k-base de A. Dans ce cas, on constate que :

$$A \cong k[X^*(\Gamma)]$$

comme k-algèbres de Hopf. Pour cela, on constate que le produit de deux caractères φ et ψ est bien donné par le produit dans l'algèbre des fonctions A sur Γ et que pour toute k-algèbre R, la structure de groupe sur $\Gamma(R)$ est bien celle de $\mathrm{Hom}(k[X^*(\Gamma)], R) = \mathrm{Hom}(X^*(\Gamma), R^\times)$: en effet, si $x, y \in \Gamma(R)$, alors pour tout $\chi \in X^*(\Gamma)$, on a bien :

$$\chi(xy) = \chi(x)\chi(y) \in R^\times.$$

Notons de plus que le groupe $X^*(\Gamma)$ est de type fini car l'algèbre A est de type fini sur $\overline{k}$: il existe donc $x_1, \ldots, x_n$ des générateurs de A, que l'on peut supposer dans $X^*(\Gamma)$, et ces x_i engendrent $X^*(\Gamma)$ car tout caractère χ est un polynôme en les x_i, et par indépendance linéaire des caractères, il est même un produit de x_i. Par le théorème de structure des groupes abéliens de type fini, on en déduit aisément que Γ est de type multiplicatif car :

$$\Gamma = \mathrm{Spec}\, k[X^*(\Gamma)].$$

Comme $X^*(\Gamma)$ est de type fini, on a un morphisme surjectif $p : \mathbb{Z}^d \longrightarrow X^*(\Gamma)$ qui induit un morphisme de groupes algébriques :

$$i : \Gamma \longrightarrow \mathrm{Spec}\, k[\mathbb{Z}^d] = \mathbb{G}_m^d.$$

Ce morphisme est une immersion fermée car le morphisme induit sur les algèbres de fonctions est surjectif. On en déduit que $2 \implies 3$.

Enfin, si Γ est un sous-groupe fermé d'un tore $\mathbb{G}_m^d$ sur k algébriquement clos, alors A est un quotient de $k[T_1,\dots,T_d,1/T_1,\dots,1/T_d]$ et donc, si $f \in A$, f est combinaison linéaire d'images de T_i^j avec $j \in \mathbb{Z}$, et ces fonctions sont des caractères sur Γ car l'inclusion de Γ dans $\mathbb{G}_m^d$ est un morphisme de groupes algébriques. □

On en déduit une dualité entre les groupes de type multiplicatif sur k et les G_k-modules continus de type fini sur $\mathbb{Z}$.

Corollaire 3.3.0.4. *Soit k un corps de caractéristique nulle. À tout G_k-module continu U de type fini sur $\mathbb{Z}$ on associe le groupe de type multiplicatif $\hat{U} = \mathrm{Spec}(\overline{k}[U])^{G_k} = \left(\mathrm{Spec}\,\overline{k}[U]\right)/G_k$, où le quotient a du sens car l'action se factorise par un groupe fini.*
Ceci définit un foncteur $\left(G_k - \mathrm{Mod}^f\right)^{\mathrm{op}} \longrightarrow \mathrm{MT}_k$ qui est un quasi-inverse du foncteur $X^*(\bullet)$ défini plus haut.
Ainsi, la catégorie des groupes de type multiplicatif sur k est anti-équivalente à la catégorie des G_k-modules continus de type fini sur $\mathbb{Z}$.

Pour mettre en valeur la dualité, on notera aussi $\hat{\Gamma}$ le groupe des caractères de Γ, de sorte que $\hat{\hat{\Gamma}} \cong \Gamma$ et $\hat{\hat{U}} \cong U$.
Bien que la dualité forme une équivalence de catégories, il n'est pas évident a priori que les suites exactes de groupes multiplicatifs induisent des suites exactes au niveau des groupes de caractères et réciproquement, car nous n'avons pas défini les suites exactes en fonction d'une structure de catégorie abélienne sur MT_k.

Proposition 3.3.0.5. *En transportant la structure de catégorie abélienne via le foncteur de dualité sur MT_k, on retrouve la même notion de suites exactes que celle définie précedemment en 3.2.0.4.*
Autrement dit, la suite $\Gamma_1 \longrightarrow \Gamma_2 \longrightarrow \Gamma_3$ est exacte si et seulement si la suite duale $\widehat{\Gamma_3} \longrightarrow \widehat{\Gamma_2} \longrightarrow \widehat{\Gamma_1}$ est exacte.

Démonstration. On commence par remarquer que si $f : \Gamma \longrightarrow \Gamma'$ est une immersion fermée, alors $X^*(\Gamma') \longrightarrow X^*(\Gamma)$ est surjective : tout caractère χ sur Γ s'étend en une fonction f sur Γ' qui est combinaison linéaire de caractères, et on utilise alors l'indépendance linéaire des caractères pour conclure qu χ est la restriction d'un de ces caractères à Γ. Réciproquement, si $U \longrightarrow V$ est surjectif, alors $\hat{V} \longrightarrow \hat{U}$ est une immersion fermée car le morphisme induit sur les algèbres de fonctions est alors surjectif.
Si $f : \Gamma \longrightarrow \Gamma'$ est un quotient, alors $X^*(\Gamma')$ s'injecte dans $X^*(\Gamma)$: on peut supposer k algébriquement clos, et si un caractère χ' de Γ' vérifie $f^*\chi' = 1$, alors topologiquement χ' est constant car f est surjective et donc χ' est le caractère trivial (il est trivial sur les k-points). Réciproquement, si $U \longrightarrow V$ est injectif, alors $\mathcal{O}(\hat{U}) \longrightarrow \mathcal{O}(\hat{V})$ aussi donc le morphisme induit sur les groupes algébriques est dominant donc c'est un quotient (voir 3.2.0.3).
Ainsi les quotients correspondent aux morphismes injectifs au niveau des groupes de caractères et les immersions fermées correspondent aux morphismes surjectifs au niveau des groupes de caractères. De plus, si $f : \Gamma_1 \longrightarrow \Gamma_2$ est un morphisme dans la catégorie MT_k, le dual de $\mathrm{Ker}(f)$ est $\mathrm{Coker}(\widehat{f})$ car ils vérifient des propriétés universelles duales.
À présent, soit $\Gamma_1 \xrightarrow{f} \Gamma_2 \xrightarrow{g} \Gamma_3$ une suite exacte de groupes de type multiplicatif sur k, et montrons que la suite duale est exacte. En étendant les scalaires à $\overline{k}$, la suite reste exacte et les duaux ne changent pas (en tant que groupes abéliens du moins). On peut donc supposer k algébriquement clos. La suite duale est clairement un complexe, et il faut donc voir que si χ est un caractère sur Γ_2 qui vérifie $f^*\chi = 1$, alors χ provient de Γ_3 par tiré en arrière par g.

On peut décomposer g en $\Gamma_2 \longrightarrow \mathrm{Im}(g) \longrightarrow \Gamma_3$ avec un quotient et une immersion fermée de sorte qu'on a une suite exacte $\Gamma_1 \xrightarrow{f} \Gamma_2 \xrightarrow{g} \mathrm{Im}(g) \longrightarrow 0$, et, si l'on sait trouver $\psi \in \widehat{\mathrm{Im}(g)}$ dont le tiré en arrière par g est χ, alors, comme $\widehat{\Gamma_3} \longrightarrow \widehat{\mathrm{Im}(g)}$ est surjectif, on aura bien ce qu'on veut.
Ainsi, on peut supposer que g est un quotient. Notons A_i l'algèbre de Hopf des fonctions sur Γ_i et B l'algèbre de Hopf des fonctions sur $\mathrm{Ker}(g)$. On a des morphismes induits :

$$\begin{array}{ccccc} A_3 & \xrightarrow{g^*} & A_2 & \xrightarrow{f^*} & A_1 \\ & & \downarrow & \nearrow & \\ & & B & & \end{array}$$

car $\Gamma_1 \longrightarrow \mathrm{Ker}(g)$ est un quotient par hypothèse d'exactitude. Puisque $f^*\chi = 1$, le diagramme ci-dessus montre que l'image de χ dans B est nulle. Or $A_i = k[\widehat{\Gamma_i}]$ et $B = k[\mathrm{Coker}\,\widehat{f}]$ par ce qui précède, donc l'image de χ dans $\mathrm{Coker}\widehat{g}$ est 1, autrement dit χ est dans l'image de $\widehat{g}$ comme souhaité.
À présent, supposons que $U \longrightarrow V \longrightarrow W$ est une suite exacte de G_k-modules continus de type fini sur $\mathbb{Z}$ et montrons que la suite duale est exacte. Comme l'exactitude se vérifie sur les $\overline{k}$-points par 3.2.0.5, on peut encore supposer k algébriquement clos. La suite duale au niveau des k-points est alors tout simplement :

$$\mathrm{Hom}(W, k^\times) \longrightarrow \mathrm{Hom}(V, k^\times) \longrightarrow \mathrm{Hom}(U, k^\times)$$

qui est exacte car $k^\times$ est un groupe abélien injectif. □

Remarque 3.3.0.6. On fait à présent quelques remarques sur cet énoncé de dualité.

— Dans la dualité précédente, les tores correspondent aux G_k-modules qui sont libres sur $\mathbb{Z}$ et les groupes finis correspondent aux G_k-modules finis sur $\mathbb{Z}$.
— Si U est un G_k-module continu de type fini sur $\mathbb{Z}$, on a une suite exacte G_k-équivariante :

$$0 \longrightarrow U_{\mathrm{tors}} \longrightarrow U \longrightarrow U/U_{\mathrm{tors}} \longrightarrow 0$$

qui donne, par dualité, pour tout Γ groupe de type multiplicatif sur k, une suite exacte $0 \longrightarrow T \longrightarrow \Gamma \longrightarrow F \longrightarrow 0$ avec T un tore et F fini. T est le tore maximal de Γ. Si k est algébriquement clos, la première suite est scindée dans la catégorie des groupes abéliens de type fini donc la seconde aussi.

Remarque 3.3.0.7. Si Γ est un groupe de type multiplicatif sur un corps k, on peut aussi voir Γ comme un module galoisien en considérant $\Gamma(k_s)$ muni de l'action naturelle de G_k. Ainsi, il est possible de définir les groupes de cohomologique $H^n(k, \Gamma)$ comme $H^n(k, \Gamma(k_s))$.
De plus, en caractéristique nulle, une suite $\Gamma_1 \longrightarrow \Gamma_2 \longrightarrow \Gamma_3$ est exacte si et seulement si la suite au niveau des k_s-points est exacte, donc une suite exacte courte de groupes de type multiplicatif induit toujours une suite exacte longue en cohomologie.
Le lien entre les modules galoisiens $\Gamma(k_s)$ et $\widetilde{\Gamma}$ est l'objet de la dualité d'Artin-Verdier.

Le calcul suivant sera utile dans la suite.

Lemme 3.3.0.8. *Soit ℓ/k une extension finie de corps de caractéristique nulle. On note Res^ℓ_k la restriction à la Weil. Soit Γ un groupe de type multiplicatif sur ℓ. On a alors un isomorphisme canonique de G_k-modules topologiques :*

$$\widehat{\mathrm{Res}^\ell_k \Gamma} \cong \mathrm{Coind}^k_\ell \widehat{\Gamma}$$

ainsi qu'un isomorphisme de G_k-modules topologiques :

$$\left(\mathrm{Res}_k^\ell \Gamma\right)(k_s) = \mathrm{Coind}_\ell^k \Gamma(k_s).$$

Démonstration. Cela peut se prouver directement ou alors se démontrer par *abstract nonsense* en contemplant le diagramme de foncteurs suivant qui commute à isomorphisme naturel près :

$$\begin{array}{ccc} \mathrm{MT}_k & \xrightarrow{\widehat{\bullet}} & \left(G_k - \mathrm{Mod}^f\right)^{\mathrm{op}} \\ \bullet\times_k \ell \downarrow \quad \uparrow \mathrm{Res}_k^\ell & & \mathrm{Res}^{G_k}_{G_\ell} \downarrow \quad \uparrow \mathrm{Coind}^{G_k}_{G_\ell} \\ \mathrm{MT}_\ell & \xrightarrow[\widehat{\bullet}]{} & \left(G_\ell - \mathrm{Mod}^f\right)^{\mathrm{op}} \end{array}$$

par unicité d'un adjoint à droite à isomorphisme naturel près. Pour ce qui est du deuxième énoncé, on a :

$$k_s \otimes_k \ell \cong k_s^{\mathrm{Hom}_k(\ell, k_s)} \cong k_s^{G_k/G_\ell}$$

de sorte que :

$$\left(\mathrm{Res}_k^\ell(\Gamma)\right)(k_s) = \Gamma(k_s \otimes_k \ell) = \prod_{\tau \in G_k/G_\ell} \Gamma(k_s) = \mathrm{Coind}_\ell^k \Gamma(k_s)$$

en vérifiant que les actions coïncident. □

Pour conclure cette partie, mentionnons enfin que si Γ est de type multiplicatif, on a un accouplement G_k-équivariant parfait modulo la torsion :

$$X^*(\Gamma) \times X_*(\Gamma) \longrightarrow \mathbb{Z}$$

qui à $\mathbb{G}_m \longrightarrow \Gamma_{\overline{k}}$ et $\Gamma_{\overline{k}} \longrightarrow \mathbb{G}_m$ associe leur composée vue dans $X^*(\mathbb{G}_m) \cong \mathbb{Z}$. En effet, il est immédiat de vérifier que :

$$X_*(\Gamma) = \mathrm{Hom}(\mathbb{G}_m, \Gamma_{\overline{k}}) = \mathrm{Hom}_{\mathrm{Grp}}(X^*(\Gamma), \mathbb{Z})$$

en passant à la catégorie duale.
Cette fois-ci, X_* ne donne pas une équivalence de catégorie car si T est le tore maximal de Γ, on a toujours $X_*(T) = X_*(\Gamma)$ de façon immédiate. En revanche, $X_*(T)$ permet notamment de classifier les sous-tores de T via la proposition suivante.

Proposition 3.3.0.9. *Soit k un corps de caractéristique nulle et Γ un tore sur k. On dispose d'une correspondance bijective entre les sous-tores de Γ et les sous $\mathbb{Q}$-espaces vectoriels de $X_*(\Gamma) \otimes \mathbb{Q}$ stables par l'action de G_k. Cette correspondance est donnée par :*

$$T \mapsto X_*(T) \otimes \mathbb{Q}.$$

Démonstration. Si T est un sous-tore de Γ, $X^*(\Gamma) \longrightarrow X^*(T)$ est surjective et équivariante donc $X_*(T) \otimes \mathbb{Q} \longrightarrow X_*(\Gamma) \otimes \mathbb{Q}$ est injective et équivariante. On note $V(T)$ son image.
Par le théorème de dualité, les sous-tores de Γ correspondent aux quotients de G_k-modules de $\widehat{\Gamma}$ qui sont libres sur $\mathbb{Z}$, qui eux correspondent aux quotients de G_k-modules de $V = \widehat{\Gamma} \otimes \mathbb{Q}$ (en effet, si $q : V \longrightarrow W$ est un tel quotient, on lui associe l'image de $\widehat{\Gamma}$ par q). Par l'accouplement parfait, cela correspond bien aux sous $\mathbb{Q}$-espaces vectoriels de $X_*(\Gamma) \otimes \mathbb{Q}$ stables par l'action de G_k. □

3.4 Dualité de Poitou-Tate pour les tores

Dans la suite, nous aurons besoin d'un résultat de dualité entre groupes de Tate-Shafarevich pour les tores. Ce théorème est un cas particulier du théorème 0.2 de [4] de Harari et Szamuely qui traite la dualité de Poitou-Tate pour les 1-motifs sur un corps de nombres. Les 1-motifs sont une classe de complexes de schémas en groupes abéliens sur $\mathrm{Spec}(K)$, avec K un corps de nombres, assez grande pour comprendre les variétés abéliennes, les tores, et les groupes abéliens de type fini muni d'une action de G_K, et stable par dualité. L'analogue pour les groupes topologiques serait par exemple la classe des groupes localement compacts pour la dualité de Pontriaguine.

Théorème 3.4.0.1. *(Poitou-Tate pour les tores) Soit K un corps de nombres et T un tore sur K. On a alors un accouplement non-dégénéré et canonique de groupes abéliens :*

$$Ш^1(T) \times Ш^2(\hat{T}) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Remarque 3.4.0.2. On ne donnera pas de preuve de cet énoncé car il n'en n'existe pas d'élémentaire avec les outils présentés jusqu'ici. Faisons tout de même quelques remarques.

— Le théorème cité de [4] donne un accouplement non-dégénéré modulo les sous-groupes divisibles, au sens où les noyaux de $Ш^1(T) \longrightarrow \mathrm{Hom}(Ш^2(\hat{T}), \mathbb{Q}/\mathbb{Z})$ et $Ш^2(\hat{T}) \longrightarrow \mathrm{Hom}(Ш^1(T), \mathbb{Q}/\mathbb{Z})$ sont des sous-groupes divisibles. Or le groupe $Ш^1(T)$ est tué par $[L : K]$ avec L/K une extension finie sur laquelle T se déploye (i.e. $T_L \cong \mathbb{G}_m^k$) par un argument de restriction-corestriction et en utilisant Hilbert 90 qui entraîne que $Ш^1(L, T_L) = 0$. Ainsi, le seul sous-groupe divisible de $Ш^1(T)$ est 0. De même, $Ш^2(L, \hat{T}) = 0$ car $\hat{T} \cong \mathbb{Z}^k$ avec l'action triviale de G_L, et par 2.6.0.6, ce groupe est nul. Ainsi, encore par restriction-corestriction, $Ш^2(K, \hat{T})$ est tué par $[L : K]$ et n'a donc que 0 comme sous-groupe divisible. On a donc bien un accouplement non-dégénéré.

— La preuve de Harari et Szamuely repose sur de la cohomologie étale et sur la dualité d'Artin-Verdier qui accouple la k-ème cohomologie d'un faisceau abélien fini $\mathcal{F}$ sur un ouvert non-vide U de $\mathrm{Spec}(\mathcal{O}_K)$ et la cohomologie *à support compact* de son dual de Cartier sur U. Il s'agit alors de passer à la limite sur les ouverts U pour obtenir un accouplement au niveau du point générique $\mathrm{Spec}(K)$.

— Il existe aussi des versions de la dualité de Poitou-Tate dans d'autres contextes, par exemple pour les groupes algébriques abéliens finis (voir le texte d'Izquierdo à ce sujet [9]).

3.5 Tores multinormiques : un résultat de Demarche et Wei

Le but de cette partie est d'étudier un type particulier de groupe de type multiplicatif : les tores multinormiques. On va notamment montrer que, sous certaines hypothèses, le premier groupe de Tate-Chafarevitch d'un tel groupe s'annule, grâce au corollaire 2.6.0.6.
Soit K un corps de nombres de clôture algébrique $\overline{K}$ et de groupe de Galois absolu G_K. On considère ici des extensions finies $L_1, \ldots, L_n$ de K et on s'intéresse au tore (voir après) T dont les K-points sont les solutions dans $\prod_i L_i^\times$ de l'équation $\prod_i N_{L_i/K}(z_i) = 1$. Un tel tore, appelé tore multinormique, et c'est un cas particulier de la construction suivante.

Définition 3.5.0.1. *Soit K un corps et A une K-algèbre de type fini. On définit le groupe algébrique $\mathrm{Res}^1_{A/K}\mathbb{G}_m$ comme le noyau de $\mathrm{Res}_{A/K}(\mathbb{G}_m)_A \longrightarrow (\mathbb{G}_m)_K$ qui est le morphisme de norme, avec $\mathrm{Res}_{A/K}$ la restriction à la Weil de A à K.*

Dans notre cas, $T = \mathrm{Res}^1_{\prod L_i/K}\mathbb{G}_m$ est décrit par la suite exacte de groupes de type multiplicatif suivante :

$$0 \longrightarrow T \longrightarrow \prod_i \mathrm{Res}^{L_i}_K \mathbb{G}_{m,L_i} \overset{\prod N_{L_i/K}}{\longrightarrow} \mathbb{G}_{m,K} \longrightarrow 0.$$

La dernière flèche est un quotient car, au niveau des $\overline{K}$-points, elle correspond à :

$$\prod_i (L_i \otimes_K \overline{K})^\times \longrightarrow \overline{K}^\times$$

c'est à dire à :

$$\prod_i \overline{K}^{\mathrm{Hom}_K(L_i,\overline{K})} \longrightarrow \overline{K}^\times.$$

Il est alors intéressant de considérer la suite exacte longue en cohomologie (voir la remarque 3.3.0.7) à la lumière du lemme 3.3.0.8 et du lemme de Shapiro 1.2.3.4 :

$$0 \longrightarrow T(K) \longrightarrow \bigoplus_i L_i^\times \overset{\prod N_{L_i/K}}{\longrightarrow} K^\times \longrightarrow H^1(K,T) \longrightarrow \bigoplus_i H^1(L_i,\mathbb{G}_m) = 0.$$

On obtient donc la proposition suivante.

Proposition 3.5.0.2. *Soit T le tore multinormique associé aux extensions L_i/K. On a alors :*

$$H^1(K,T) = \frac{K^\times}{N(L_1/K)N(L_2/K)\dots N(L_n/K)}$$

avec $N(L_i/K)$ l'image du morphisme norme $N_{L_i/K}$. On a aussi :

$$Ш^1(K,T) = \mathrm{Ker}\left(\frac{K^\times}{N(L_1/K)\dots N(L_n/K)} \longrightarrow \prod_{v\in\Omega_K} \frac{K_v^\times}{N((L_1)_v/K)\dots N((L_n)_v/K)} \right)$$

avec $(L_i)_v = L_i \otimes_K K_v$, qui est un produit d'extensions finies de K_v.

Ainsi, l'annulation du groupe $Ш^1(K,T)$ revient à dire que *le fait d'être une norme pour les extensions L_i se vérifie localement*. C'est donc une propriété d'intérêt pour la conjecture de Kato et Kuzumaki dans le cas $q = 1$. L'article de Demarche et Wei, [2], donne alors des conditions d'annulation de ce groupe.
Pour comprendre cela, commençons par considérer la suite exacte duale de G_K-modules topologiques. Elle correspond à :

$$0 \longrightarrow \mathbb{Z} \longrightarrow \prod_i \mathrm{Coind}^K_{L_i}\mathbb{Z} \longrightarrow \widehat{T} \longrightarrow 0 \quad (*)$$

par le lemme 3.3.0.8. Rappelons que $\mathrm{Coind}^K_{L_i}\mathbb{Z}$ est isomorphe au module de permutation $\mathbb{Z}[G_K/G_{L_i}]$ et en déroulant les définitions, on voit bien que le premier morphisme de cette suite duale envoie 1 sur $\sum_i \sum_{x\in G_K/G_{L_i}} x$. On en déduit que cette suite est scindée dans la catégorie des groupes abéliens, ce qui justifie que $\widehat{T}$ est libre sur $\mathbb{Z}$ et donc que T est bien un tore.
A priori, $\widehat{T}$ n'est pas un G_K-module de permutation et donc on ne peut pas directement utiliser le corollaire 2.6.0.6. Le lemme suivant donne une condition suffisante pour qu'un quotient comme on rencontre ici soit un module de permutation. La condition n'est pas remplie ici, sauf si l'un des L_i est K, mais on va voir comment forcer à obtenir cette condition sous de bonnes hypothèses.

Lemme 3.5.0.3. *Soit G un groupe profini et X un ensemble fini non-vide muni d'une action de G. On pose :*

$$\alpha = \sum_{x \in X} x \in \mathbb{Z}[X].$$

Si X possède un point fixe par G, p, alors on a un isomorphisme de G-modules topologiques :

$$\mathbb{Z}[X]/\mathbb{Z}\alpha \cong \mathbb{Z}[X \setminus \{p\}]$$

et la suite $0 \longrightarrow \mathbb{Z}\alpha \longrightarrow \mathbb{Z}[X] \longrightarrow \mathbb{Z}[X \setminus \{p\}] \longrightarrow 0$ est scindée dans la catégorie des G-modules topologiques.

Démonstration. Notons déjà que α est fixé par G donc le quotient $M = \mathbb{Z}[X]/\mathbb{Z}\alpha$ est bien un G-module. S'il existe $p \in X$ fixé par G, alors la famille $(x)_{x \neq p} \cup (\alpha)$ est une $\mathbb{Z}$-base de $\mathbb{Z}[X]$, et induit une décomposition :

$$\mathbb{Z}[X] = \mathbb{Z}[X \setminus \{p\}] \oplus \mathbb{Z}\alpha$$

et chaque facteur de cette décomposition est stable par G, d'où la conclusion. □

L'idée de Demarche et Wei pour obtenir l'annulation de $Ш^2_\omega(K, \widehat{T})$ sous certaines hypothèses de disjonction linéaire des L_i est de regrouper les L_i en deux familles. Pour l'instant, faisons cela de façon arbitraire : on considère une partition $\{1, \dots, n\} = I \sqcup J$ avec I et J *non-vides*, et on forme les compositums L_I et L_J des L_i pour $i \in I$ et pour $i \in J$ respectivement. On considère aussi E_I et E_J leurs clôtures galoisiennes respectives.
On observe alors que G_K/G_{L_i}, en tant que G_{L_I}-ensemble, avec $i \in I$, possède un point fixe, à savoir la classe de l'élément neutre. Ainsi, par le lemme 3.5.0.3, on en déduit que $\widehat{T}$ est un G_{L_I} (resp. G_{L_J}, resp. G_{E_I}, resp. G_{E_J}) module de permutation, et que la suite exacte duale (∗) est scindée dans la catégorie des modules topologiques sur ces groupes-ci.
En particulier, ceci donne l'annulation de $Ш^2_\omega(U, \widehat{T})$ pour $U = L_I, L_J, E_I$ ou E_J. Ainsi, si on parvient à trouver des hypothèses sous-lesquelles le morphisme canonique de restriction :

$$H^2(K, \widehat{T}) \longrightarrow H^2(L_I, \widehat{T}) \oplus H^2(E_J, \widehat{T})$$

est injectif, on aura obtenu $Ш^2_\omega(K, \widehat{T}) = 0$. C'est l'objet de la preuve du théorème suivant.

Théorème 3.5.0.4. *(Demarche et Wei)*
Soit K un corps de nombres et $L_1, \dots, L_n$ des extensions finies de K. On considère le tore multinormique T défini plus haut, dont les K-points sont les solutions de l'équation multinormique $\prod_i N_{L_i/K}(z_i) = 1$.
S'il existe une partition $I \sqcup J = \{1, \dots, n\}$ telle que, avec les notations précédentes, $L_I \cap E_J = K$, alors on a :

$$Ш^2_\omega(K, \widehat{T}) = 0.$$

Par dualité de Poitou-Tate 3.4.0.1, on a donc :

$$Ш^1(K, T) = 0.$$

Démonstration. Commençons par rappeler que si G est un groupe profini et A un module de permutation de type fini sur $\mathbb{Z}$, alors $H^1(G, A) = 0$: en effet, par Shapiro, cela revient à établir que $H^1(G, \mathbb{Z}) = 0$, or $H^1(G, \mathbb{Z})$ s'identifie aux morphismes continus de G vers $\mathbb{Z}$, et un tel morphisme se factorise par son noyau qui est ouvert donc d'indice fini, et il n'y a qu'un seul morphisme d'un

groupe fini vers $\mathbb{Z}$: le morphisme trivial.
Comme vu précedemment, il suffit de montrer que le morphisme canonique de restriction :

$$H^2(K, \widehat{T}) \longrightarrow H^2(L_I, \widehat{T}) \oplus H^2(E_J, \widehat{T})$$

est injectif. Or on a $H^1(E_J, \widehat{T}) = 0$ car $\widehat{T}$ est un module de permutation sur G_{E_J}. Ainsi, la suite spectrale de Hoschild-Serre donne une suite exacte d'inflation restriction en degré 2 :

$$0 \longrightarrow H^2\left(E_J/K, \widehat{T}^{G_{E_J}}\right) \longrightarrow H^2(K, \widehat{T}) \longrightarrow H^2(E_J, \widehat{T}).$$

On est donc ramenés à prouver l'injectivité de la composée suivante :

$$H^2\left(E_J/K, \widehat{T}^{G_{E_J}}\right) \longrightarrow H^2(K, \widehat{T}) \longrightarrow H^2(L_I, \widehat{T}).$$

C'est ici qu'on utilise le fait que $L_I \cap E_J = K$: ceci assure que $L_I \otimes_K E_J \cong L_I E_J$ et que $\mathrm{Gal}(L_I E_J/L_I) \cong \mathrm{Gal}(E_J/K)$ par un argument classique de théorie de Galois en utilisant que E_J/K est galoisienne, et que le produit d'un sous-groupe distingué par un sous-groupe est un sous-groupe. On a ainsi :

$$H^2\left(E_J/K, \widehat{T}^{G_{E_J}}\right) \cong H^2\left(L_I E_J/L_I, \widehat{T}^{G_{E_J}}\right)$$

et on peut alors contempler le diagramme commutatif suivant :

$$\begin{array}{ccccc}
H^2\left(E_J/K, \widehat{T}^{G_{E_J}}\right) & \longrightarrow & H^2(K, \widehat{T}) & \longrightarrow & H^2(L_I, \widehat{T}) \\
|| & & & & || \\
H^2\left(L_I E_J/L_I, \widehat{T}^{G_{E_J}}\right) & \longrightarrow & H^2\left(L_I, \widehat{T}^{G_{E_J}}\right) & \longrightarrow & H^2(L_I, \widehat{T})
\end{array}$$

où le morphisme du dessous à gauche est donné par inflation, car $\left(\widehat{T}^{G_{E_J}}\right)^{G_{L_I E_J}} = \widehat{T}^{G_{E_J}}$.
Il faut donc montrer que la composée de la ligne inférieure de ce diagramme est injective. On montre que chacune des deux flèches est injective. D'abord, $H^1(L_I E_J, \widehat{T}^{G_{E_J}}) = 0$ car $\widehat{T}^{G_{E_J}} \cong \mathbb{Z}^N$ avec action triviale comme $G_{L_I E_J}$-module. Ainsi, la suite spectrale d'Hoschild-Serre donne l'injectivité de la première flèche. Pour la seconde, il suffit de constater qu'elle est induite par l'inclusion $\widehat{T}^{G_{E_J}} \subseteq \widehat{T}$ qui admet une rétraction G_{L_I}-équivariante, comme on va le voir tout de suite. Posons :

$$A = \prod_i \mathrm{Coind}_{G_{L_i}}^K \mathbb{Z} = \prod_i \mathbb{Z}[G_K/G_{L_i}].$$

Puisque $H^1(E_J, \mathbb{Z}) = 0$, on a le diagramme commutatif à lignes exactes suivant en prenant les points fixes par G_{E_J} dans la suite exacte $(*)$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & A & \longrightarrow & \widehat{T} & \longrightarrow & 0 \\
 & & || & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & A^{G_{E_J}} & \longrightarrow & \widehat{T}^{G_{E_J}} & \longrightarrow & 0
\end{array}$$

et on souhaite voir que $\widehat{T}^{G_{E_J}} \hookrightarrow \widehat{T}$ admet un rétract dans la catégorie des G_{L_I}-modules topologiques. Par un exercice de chasse au diagramme, on se convainc qu'il suffit de voir que $A^{G_{E_J}} \hookrightarrow A$ admet un

rétract dans cette même catégorie. Pour enfin obtenir ceci, on note que $G_{E_J} G_{L_i} = G_K$ pour tout $i \in I$ et donc G_{E_J} agit transitivement sur G_K/G_{L_i} et donc $\mathbb{Z}[G_K/G_{L_i}]^{G_{E_J}} = \mathbb{Z}\alpha_i$ avec $\alpha_i = \sum_{x \in G_K/G_{L_i}} x$. On a donc :

$$A^{G_{E_J}} = \bigoplus_{i \in I} \mathbb{Z}\alpha_i \oplus \bigoplus_{j \in J} \mathbb{Z}[G_K/G_{L_j}]^{G_{E_J}}.$$

Le premier gros facteur est bien un facteur direct de A comme G_{L_I}-modules par le lemme 3.5.0.3 appliqué à chaque $\mathbb{Z}[G_K/G_{L_i}]$ car G_K/G_{L_i} possède un point fixe sous l'action de G_{L_I}. Ensuite, pour chaque $j \in J$, $\mathbb{Z}[G_K/G_{L_j}]^{G_{E_J}} = \mathbb{Z}[G_K/G_{L_j}]$ car G_{E_J} agit trivialement sur G_K/G_{L_j} puisque $G_{E_J} \subseteq G_{L_j}$ et G_{E_J} est distingué dans G_K. Ceci permet de conclure. □

3.6 Tores multinormiques infinis et une généralisation du théorème de Demarche et Wei

Soit K un corps de nombres de clôture algébrique $\overline{K}$. Dans cette partie, on souhaite généraliser le théorème d'annulation de Demarche et Wei à des tores multinormiques définis par une infinité d'extensions finies de K. Cette nouvelle formulation permettra de comprendre la preuve d'Izquierdo du fait que les corps de nombres totalement imaginaires sont C_1^1 (voir 9.1).

Définition 3.6.0.1. *Soit $\mathcal{L}$ une famille non-vide d'extensions finies de K. On définit le tore multinormique $T_{\mathcal{L}}$ comme le G_K-module topologique noyau du morphisme surjectif suivant :*

$$\bigoplus_{L \in \mathcal{L}} \mathrm{Coind}_L^K \overline{K}^\times \longrightarrow \overline{K}^\times.$$

Dans cette définition, $T_{\mathcal{L}}$ est un module galoisien et non un groupe algébrique comme dans le cas d'un nombre fini d'extensions.
Puisque la cohomologie des groupes profinis commute aux colimites filtrantes par 1.2.1.9, la proposition 3.5.0.2 reste valable avec une preuve similaire. On a donc :

$$H^1(K, T_{\mathcal{L}}) = \frac{K^\times}{\langle N(L/K) \mid L \in \mathcal{L} \rangle}$$

et :

$$Ш^1(K, T_{\mathcal{L}}) = \mathrm{Ker}\left(\frac{K^\times}{\langle N(L/K) \mid L \in \mathcal{L} \rangle} \longrightarrow \prod_{v \in \Omega_K} \frac{K_v^\times}{\langle N(L_v/K_v) \mid L \in \mathcal{L} \rangle} \right).$$

Si v est une place de K, on note $\mathcal{L}_v$ l'ensemble des extensions finies de L_v qui apparaissent comme facteurs des algèbres étales L_v avec $L \in \mathcal{L}$, de sorte que :

$$Ш^1(K, T_{\mathcal{L}}) = \mathrm{Ker}\left(H^1(K, T_{\mathcal{L}}) \longrightarrow \prod_v H^1(K_v, T_{\mathcal{L}_v}) \right).$$

On peut tout de suite faire quelques remarques de fonctorialité : si $\mathcal{L} \subseteq \mathcal{L}'$, alors on a un morphisme surjectif $H^1(K, T_{\mathcal{L}}) \longrightarrow H^1(K, T_{\mathcal{L}'})$ et donc un morphisme $Ш^1(K, T_{\mathcal{L}}) \longrightarrow Ш^1(K, T_{\mathcal{L}'})$.
De plus, si on ajoute à $\mathcal{L}$ des extensions qui contiennent des extensions de $\mathcal{L}$, le groupe $H^1(K, T_{\mathcal{L}})$ ainsi que les groupes $H^1(K_v, T_{\mathcal{L}_v})$ restent inchangés. On peut donc supposer que $\mathcal{L}$ est stable par passage à des sur-extensions.

Définition 3.6.0.2. *Un système d'extensions $\mathcal{L}$ de K est une famille non-vide d'extensions finies de K stable par passage à une sur-extension. Un tel système est dit séparé si pour tout $L \in \mathcal{L}$ il existe $L' \in \mathcal{L}$ telle que :*

$$L \cap L' = K.$$

Remarque 3.6.0.3. De façon équivalente, on peut considérer des systèmes non-vides $\mathcal{U}$ de sous-groupes ouverts de G_K stables par passage à un sous-groupe. Un tel système est alors *séparé* si pour tout $U \in \mathcal{U}$, il existe $U' \in \mathcal{U}$ tel que :

$$\langle U, U' \rangle = G_K.$$

Le lemme de compacité suivant ramène l'étude des tores multinormiques infinis à celle des tores multinormiques finis de Demarche et Wei. La preuve est adaptée de l'article d'Izquierdo [10].

Lemme 3.6.0.4. *(Lemme de compacité)*
Soit K un corps de nombres et $\mathcal{L}$ un système d'extensions de K. Le morphisme canonique :

$$\operatorname{colim}_{\mathcal{F} \subseteq \mathcal{L}} Ш^1(K, T_{\mathcal{F}}) \longrightarrow Ш^1(K, T_{\mathcal{L}})$$

est surjectif, avec la colimite qui porte sur les parties finies non-vides de $\mathcal{L}$.

Démonstration. Puisque $\mathcal{L}$ est non-vide, il existe $L_0 \in \mathcal{L}$. Soit alors $x \in K^\times$ dont la classe $[x] \in H^1(K, T_{\mathcal{L}})$ est dans $Ш^1(K, T_{\mathcal{L}})$.
Ainsi, pour toute place v, on trouve des extensions finies $L_i^{(v)} \in \mathcal{L}$ de K pour lesquelles $x \in N((L_i^{(v)})_v / K_v)$. L'astuce est alors de remarquer que pour presque toute place v, v est finie, non-ramifiée dans L_0 et x est une unité pour v, de sorte que $x \in N((L_0)_v / K_v)$. On en déduit qu'il existe une famille finie d'extensions finies $\mathcal{F} \subseteq \mathcal{L}$ non-vide telle que, pour toute place v, on ait :

$$x \in \langle N(F_v / K_v) \mid F \in \mathcal{F} \rangle$$

en prenant les $L_i^{(v)}$ et L_0. □

On peut alors démontrer le théorème suivant qui généralise une forme faible du théorème d'annulation de Demarche et Wei 3.5.0.4. On pourrait sûrement trouver des hypothèses plus faibles sur le système $\mathcal{L}$ mais cette version du théorème suffit à nos applications.

Théorème 3.6.0.5. *Soit K un corps de nombres et $\mathcal{L}$ un système d'extensions séparé. Alors :*

$$Ш^1(K, T_{\mathcal{L}}) = 0.$$

Démonstration. Il suffit de voir que la colimite du lemme de compacité est nulle, or pour tout sous-ensemble fini non-vide $\mathcal{F}$ de $\mathcal{L}$, puisque $\mathcal{L}$ est séparé, on trouve F' une extension de K dans $\mathcal{L}$ linéairement disjointe de la clôture galoisienne du compositum des extensions de $\mathcal{L}$, et en considérant $\mathcal{F}' = \mathcal{F} \cup \{F'\}$, le théorème d'annulation de Demarche et Wei 3.5.0.4 donne :

$$Ш^1(K, T_{\mathcal{F}'}) = 0.$$

Or ces groupes là sont cofinaux dans le diagramme qui donne la colimite, d'où la conclusion. □

Si $\mathcal{L}$ est un système d'extensions de K et E/K est une extension finie, on obtient un système d'extensions de E en posant :

$$\mathcal{L}^E = \{L \in \mathcal{L} \mid E \subseteq L\}.$$

Pour que cela ait du sens, il faut que tout soit plongé dans $\overline{K}$ une clôture algébrique de K. On a alors des morphismes de restriction et corestriction :

$$Ш^1(K, T_{\mathcal{L}}) \underset{\text{Cor}}{\overset{\text{Res}}{\rightleftarrows}} Ш^1(E, T_{\mathcal{L}^E})$$

qui vérifient $\text{Cor} \circ \text{Res} = [E : K]\text{id}$. La corestriction est induite par la norme $N_{E/K}$ tandis que la restriction est induite par l'inclusion $K^\times \subseteq E^\times$.

Chapitre 4

K-théorie de Milnor et formes quadratiques

Dans ce chapitre, on présente une suite d'invariants associés à des corps quelconques par Milnor, les groupes de K-théorie de Milnor, et on relie leur version "modulo 2" à la théorie des formes quadratiques. Pour la K-théorie de Milnor, on se base sur le livre de Gille et Szamuely [20], sans donner les preuves de tous les résultats. On renvoie donc le lecteur à cet ouvrage pour plus de détails.

4.1 Définition de la K-théorie de Milnor d'un corps

Soit k un corps. Milnor associe à k un anneau gradué de K-théorie :

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

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 $K_1(k) = k^\times$. Cette définition ad-hoc fait en fait partie d'un contexte plus général de K-théorie algébrique qui contient la K-théorie de Milnor.
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.
Mentionnons rapidement les propriétés de base de cet anneau.

Lemme 4.1.0.1. *Soient $a_1, \dots, a_n \in k^\times$ et $a, b \in k^\times$. Les faits suivants sont vrais.*

1. *Si l'un des a_i vaut 1, alors $\{a_1, \dots, a_n\} = 0$.*
2. *On a $\{a, -a\} = 0$.*
3. *On a $\{a, b\} = -\{b, a\}$.*
4. *On a $\{a, a\} = \{-1, a\} = \{a, -1\}$.*
5. *L'algèbre $K_*(k)$ est commutative au sens gradué, c'est à dire que $uv = (-1)^{mn}vu$ pour $u \in K_m(k)$ et $v \in K_n(k)$.*
6. *S'il existe $I \subseteq \{1, \dots, n\}$ non-vide tel que $\sum_{i\in I} a_i \in \{0, 1\}$, alors $\{a_1, \dots, a_n\} = 0$.*

Démonstration. Le premier point vient du fait que 1 est le zéro du $\mathbb{Z}$-module $k^\times$.
On observe, pour le second point (on peut supposer $a \neq 1$)

$$0 = \left\{a^{-1}, 1-a^{-1}\right\} = -\left\{a, 1-a^{-1}\right\} = -\left\{a, \frac{a-1}{a}\right\} = -\left\{a, \frac{1-a}{-a}\right\} = -\{a, 1-a\} + \{a, -a\} = \{a, -a\}.$$

On en déduit que :

$$0 = \{ab, -ab\} = \{a, -a\} + \{a, b\} + \{b, a\} + \{b, -b\} = \{a, b\} + \{b, a\}.$$

Ensuite :

$$\{a, a\} + \{a, -1\} = \{a, -a\} = 0$$

donc $\{a, a\} = -\{a, -1\}$ or $2\{a, -1\} = \left\{a, (-1)^2\right\} = 0$ donc on peut retirer le signe.
La relation de commutativité au signe près découle directement du troisième point.
Voyons enfin le dernier point. Par commutativité, on peut supposer $\sum_{i=1}^{k} a_i \in \{0, 1\}$ avec $k \geq 1$. Le cas $k = 2$ étant connu, on suppose $k \geq 3$ et que l'hypothèse de récurrence pour $k - 1$ est connue. Posons $S = a_1 + a_2$. Si $S = 0$, c'est le point 2 qui conclut. Sinon, on a $\frac{a_1}{S} + \frac{a_2}{S} = 1$ donc :

$$0 = \left\{\frac{a_1}{S}, \frac{a_2}{S}\right\} = \{a_1, a_2\} - \{a_1, S\} - \{a_2, S\} + \{S, S\}.$$

On multiplie cette égalité à droite par $\{a_3, \ldots, a_n\}$ et les trois derniers termes sont nuls par hypothèse de récurrence puisque $S + a_3 + \cdots + a_n \in \{0, 1\}$, et donc finalement :

$$\{a_1, \ldots, a_n\} = 0.$$

□

Exemple 4.1.0.2. Soit k un corps fini. Alors pour tout $q \geq 2$ on a :

$$K_q(k) = 0.$$

Démonstration. Il suffit clairement de montrer que $K_2(k) = 0$. Choisissons a un générateur de $k^\times$ de sorte que $K_2(k)$ est engendré par $\{a, a\} = \{-1, a\}$. Notons p la caractéristique de k et :

$$m = |k| = p^r$$

avec $r \geq 1$. Si $p = 2$, on a $-1 = 1$ donc $\{-1, a\} = 0$ et $K_2(k) = 0$. Supposons maintenant p impair. On a :

$$2\{-1, a\} = \{1, a\} = 0$$

donc $K_2(k)$ est d'ordre au plus 2. Ensuite, remarquons que :

$$-1 = a^{\frac{m-1}{2}}$$

et donc $\{-1, a\} = \frac{m-1}{2}\{a, a\} = \frac{m-1}{2}\{-1, a\}$ de sorte que si $m \equiv 1\ [4]$, on a $\{-1, a\} = 0$ comme voulu. Supposons à présent $m \equiv 3\ [4]$ de sorte que $p \equiv 3\ [4]$ et r est impair, et par la seconde loi complémentaire de la réciprocité quadratique, 2 n'est pas un carré modulo p et n'est pas non plus un carré dans k car r est impair. Or on a $\frac{1}{2} + \frac{1}{2} = 1$ donc $\left\{2^{-1}, 2^{-1}\right\} = 0$ et donc $\{2, 2\} = 0$. Puisque 2 n'est pas un carré, on écrit $2 = \alpha^i$ avec i impair et ainsi :

$$i^2\{\alpha, \alpha\} = 0$$

donc $\{\alpha, \alpha\} = 0$ et on conclut. □

4.2 Morphismes résiduels et morphismes de spécialisation

Ici, K est un corps de valuation discrète v, de corps résiduel k et d'anneau des entiers R. Il est possible de relier la K-théorie de K et celle de k grâce à deux types de morphismes, les morphismes résiduels et de spécialisation. On note $\overline{a}$ la réduction dans k d'un élément $a \in R$.

On ne se réferera pas à la construction explicite de ces morphismes dans la suite, mais expliquons tout de même rapidement de quoi il retourne. On utilise une idée de Serre : on construit d'abord un anneau $K_*(k)[x]$ obtenu en ajoutant à l'anneau $K_*(k)$ la variable x avec la contrainte que $\alpha x = -x\alpha$ pour tout $\alpha \in K_1(k)$. On obtient ainsi un anneau gradué avec x en degré 1, et on quotiente cet anneau par $x^2 - \{-1\}x$ pour obtenir un anneau noté $K_*(k)[\zeta]$, avec ζ l'image de x. La graduation de cet anneau est alors la suivante :

$$K_*(k)[\zeta] = \bigoplus_{n \geq 0} L_n$$

avec $L_n = K_n(k) \oplus \zeta K_{n-1}(k)$ pour $n \geq 1$ et $L_0 = K_0(k) = \mathbb{Z}$.
Fixons alors π une uniformisante de K et construisons le morphisme suivant :

$$K^\times \xrightarrow{d_\pi} L_1 \subseteq K_*(k)[\zeta]$$

qui envoie $\pi^k u$ sur le couple $(\overline{u}, \zeta k) \in L_1$, avec u une unité et $k \in \mathbb{Z}$. Un calcul détaillé dans [20] montre que $d_\pi(a)d_\pi(1-a) = 0$ pour tout $a \in K \setminus \{0,1\}$ de sorte que d_π induit un morphisme d'anneaux gradués :

$$K_*(K) \xrightarrow{d_\pi} K_*(k)[\zeta].$$

Ainsi, pour tout $n \geq 0$, on obtient un morphisme :

$$K_n(K) \xrightarrow{s_\pi} K_n(k)$$

dit de *spécialisation* et un morphisme :

$$K_n(K) \xrightarrow{\partial} K_{n-1}(k)$$

dit de *résidu* (si $n \geq 1$). On vérifie alors que ∂ ne dépend pas de π.
On a d'ailleurs les formules suivantes, qui décrivent entièrement ∂ et s_π car les symboles de la forme donnée dans la proposition engendrent la K-théorie de Milnor.

Proposition 4.2.0.1. *Soit π une uniformisante, $u_1, \ldots, u_n$ des unités et $i_1, \ldots, i_n \in \mathbb{Z}$. On a alors :*

$$\partial\{\pi, u_2, \ldots, u_n\} = \{\overline{u_2}, \ldots, \overline{u_n}\}$$

et :

$$s_\pi\left\{\pi^{i_1}u_1, \ldots, \pi^{i_n}u_n\right\} = \{\overline{u_1}, \ldots, \overline{u_n}\}.$$

On définit ensuite les groupes d'unités en K-théorie de Milnor. On utilise les notations usuelles : $U^0(K) = R^\times$, $U^1(K) = 1 + \pi R$.

Définition 4.2.0.2. *On définit le groupe $U_n(K)$ comme le sous-groupe de $K_n(K)$ engendré par les symboles $\{u_1, \ldots, u_n\}$ avec $u_i \in R^\times$, et le groupe $U_n^1(K)$ comme le sous-groupe de $K_n(K)$ engendré par les symboles $\{x_1, \ldots, x_n\}$ avec $x_1 \in U^1(K)$. Par convention, $U_0^1(K) = 0$.*

On peut alors montrer, en se ramenant au cas $n = 2$, que :

$$U_n^1(K) \subseteq U_n(K)$$

bien que ça ne saute pas aux yeux. On montre alors qu'on dispose de deux suites exactes qui relient la K-théorie de K à celle de k.

Proposition 4.2.0.3. *Soit K un corps de valuation discrète de corps résiduel k. On a deux suites exactes :*

$$0 \longrightarrow U_n(K) \longrightarrow K_n(K) \xrightarrow{\partial} K_{n-1}(k) \longrightarrow 0$$

et :

$$0 \longrightarrow U_n^1(K) \longrightarrow U_n(K) \xrightarrow{s} K_n(k) \longrightarrow 0$$

où s est la restriction d'un morphisme de spécialisation s_π à $U_n(K)$, qui ne dépend pas de l'uniformisante choisie.

Notons que pour $n = 1$, le morphisme ∂ est donné par la valuation et donc la première suite exacte donne simplement $K^\times/\mathcal{R}^\times \cong \mathbb{Z}$. La deuxième suite exacte, donne, toujours pour $n = 1$:

$$R^\times/(1 + \pi R) \cong k^\times.$$

Proposition 4.2.0.4. *Soit K un corps de valuation discrète complet de corps résiduel k et soit d un entier non-nul dans k. Pour tout choix d'uniformisante π de K et pour tout $n \geq 1$, on a alors un isomorphisme :*

$$\frac{K_n(K)}{dK_n(K)} \xrightarrow{s_\pi \oplus \partial} \frac{K_n(k)}{dK_n(k)} \oplus \frac{K_{n-1}(k)}{dK_{n-1}(k)}.$$

Démonstration. La surjectivité est claire au vu de la proposition précédente. Voyons l'injectivité : si $\alpha \in K_n(K)$ est envoyé sur 0 dans le terme de droite, alors par surjectivité de s_π et de ∂, on a :

$$\alpha \in \mathrm{Ker}(s_\pi) + dU_n(K)$$

et :

$$\alpha \in \mathrm{Ker}(\partial) + dK_n(K).$$

Par la deuxième affirmation, sans changer la classe de α modulo d et tout en gardant la première affirmation, on peut supposer $\partial\alpha = 0$, et ainsi $\alpha \in U_n(K)$. On a donc :

$$\alpha \in U_n^1(K) + dU_n(K)$$

et le groupe $U_n^1(K)$ est divisible par d car $U^1(K)$ l'est, puisque K est *complet* et d est non-nul dans k (on utilise simplement le lemme de Hensel). □

4.3 Morphismes de norme

Si L/K est une extension finie de corps, il est possible de définir des morphismes :

$$N_{L/K} : K_n(L) \longrightarrow K_n(K)$$

pour tout $n \geq 0$. Concrètement, on a le théorème suivant.

Théorème 4.3.0.1. *Pour chaque extension finie L/K de corps, et pour tout $n \geq 0$, il existe un morphisme :*

$$N_{L/K} : K_n(L) \longrightarrow K_n(K)$$

de sorte qu'on ait les points suivants.

- *Pour $n = 0$, le morphisme $N_{L/K} : K_0(L) \longrightarrow K_0(K)$ est la multiplication par $[L : K]$ sur $\mathbb{Z}$.*
- *Pour $n = 1$, c'est le morphisme de norme $L^\times \longrightarrow K^\times$.*
- *On a une formule de projection :*

$$N_{L/K}(\alpha)\beta = N_{L/K}(\alpha\beta_{|L}) \in K_{n+m}(K)$$

  pour $\alpha \in K_n(L)$, $\beta \in K_m(K)$, en notant $\beta_{|L}$ l'image de β dans $K_m(L)$.
- *Les normes se composent bien vis à vis des tours d'extensions, au sens où si $M/L/K$ est une tour d'extensions finies, on a $N_{M/K} = N_{L/K} \circ N_{M/L}$ en K-théorie.*

Un tel jeu de morphismes est alors entièrement caractérisé par ces propriétés.

La construction de tels morphismes n'est pas évidente. Une vague idée de construction est de commencer par le cas des extensions de la forme $K(P)/K$ avec P un point fermé de $\mathbb{P}^1_K$ (c'est à dire des extensions monogènes) en utilisant le théorème de Milnor qui relie la K-théorie du corps des fonctions de $\mathbb{P}^1_K$, à savoir $K(t)$ à la K-théorie des corps résiduels en les points fermés de $\mathbb{P}^1_K$, puis de montrer que ce choix ne dépend pas du point choisi avec un résultat de Kato. Encore une fois, les détails sont dans le chapitre 7 de [20].

Dans le cas de corps de valuation discrète complets, on a une compatibilité entre les morphismes résiduels et de spécialisation avec la norme, et la norme préserve les groupes d'unités définis dans 4.2.0.2.

Proposition 4.3.0.2. *Soit L/K une extension finie de corps complets à valuation discrète, et soit ℓ/k l'extension résiduelle associée et $e(L/K)$ l'indice de ramification associé. On a alors un diagramme commutatif :*

$$\begin{array}{ccc} K_n(L) & \xrightarrow{\partial} & K_{n-1}(\ell) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{\ell/k}} \\ K_n(K) & \xrightarrow[\partial]{} & K_{n-1}(k) \end{array}$$

De plus, si π_L et π_K sont deux uniformisantes de L et K, alors, en notant $-\pi_K = u(-\pi_L)^e$ avec u une unité de L, on a pour tout $\alpha \in K_n(L)$:

$$s_{\pi_K} \circ N_{L/K}(\alpha) = eN_{\ell/k} \circ s_{\pi_L}(\alpha) + N_{\ell/k} \circ \partial(\{u\}\alpha).$$

Si $\alpha \in U_n(K)$, le deuxième terme de cette somme est nul car $\{u\}\alpha \in U_{n+1}(L)$ et on a donc un diagramme commutatif indépendant des choix d'uniformisantes :

$$\begin{array}{ccc} U_n(L) & \xrightarrow{s} & K_n(\ell) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle e(L/K)N_{\ell/k}} \\ U_n(K) & \xrightarrow[s]{} & K_n(k) \end{array}$$

Le premier énoncé est délicat et repose sur la construction des morphismes normes (voir [20]). Le deuxième découle directement du premier grâce à la formule suivante :

$$s_{\pi_K}(\alpha) = \partial(\{-\pi_K\}\alpha)$$

pour tout $\alpha \in K_n(K)$.

4.4 Formes quadratiques sur un corps

On fixe k un corps de *caractéristique différente de* 2. Dans ce contexte, la donnée d'une forme quadratique q sur un k espace vectoriel V (qui sera toujours de *dimension finie*) équivaut à la donnée d'une forme bilinéaire symétrique sur V. On parle alors de l'espace quadratique (V,q) et ces espaces forment une catégorie dont les morphismes sont les applications linéaires qui préservent la forme quadratique, appelés isométries.
On dira abusivement que deux formes quadratiques q_1, q_2 sont isomorphes, en notant cela $q_1 \cong q_2$ pour dire que les espaces quadratiques associés sont isomorphes.
Une forme quadratique q est *régulière* si la forme bilinéaire symétrique associée l'est (on dit aussi qu'elle est non-dégénérée) et on dit qu'elle est anisotrope si elle n'a pas de zéro non-trivial, et qu'elle est isotrope dans le cas contraire. Un résultat élémentaire qui remonte à Gauss affirme que tout espace quadratique (V,q) est somme directe orthogonale de droites quadratiques, autrement dit que q est isomorphe à une forme quadratique diagonale, notée $\langle a_1,\dots,a_n\rangle$ qui est la forme quadratique associée au polynôme homogène de degré 2 :

$$\sum_i a_i X_i^2.$$

Notes que seule la classe de a_i dans $k/(k^\times)^2$ est importante pour la définition de cette forme à isomorphisme près puisque si on change a_i en $t_i^2 a_i$, un changement de variable $Y_i = t_i X_i$ montre qu'on reste dans la même classe d'équivalence.
Si q et q' sont deux formes quadratiques, on note $q \oplus q'$ leur somme directe orthogonale et $q \otimes q'$ leur produit tensoriel, qui est une forme de dimension $\dim q \times \dim q'$ qui s'obtient en prenant le produit tensoriel des matrices de q et q' dans des bases.
On rappelle que le *discriminant* d'une forme quadratique q est le déterminant de sa matrice de Gram $(B(x_i,x_j))$ dans n'importe quelle base $\underline{x}$, avec B la forme bilinéaire symétrique associée à q, et que ce déterminant est bien défini dans $k/(k^\times)^2$. On le note $\mathrm{Disc}(q)$.
On rappelle ensuite le théorème d'annulation de Witt selon lequel, si trois formes quadratiques vérifient :

$$q_1 \oplus q_2 \cong q_1 \oplus q_3$$

alors $q_2 \cong q_3$.

4.5 Anneau de Witt

On peut considérer l'ensemble $\hat{W}_{\mathrm{mon}}(k)$ des formes quadratiques non-dégénérées sur k à isomorphisme près (qui est bien un ensemble puisqu'il suffit de prendre des matrices diagonales) et le munir de l'opération de somme directe orthogonale pour en faire un *monoïde commutatif* dont le neutre est la forme nulle de dimension 0, notée 0 ou $\langle\rangle$.
La fameuse construction de Grothendieck permet d'associer à ce monoïde commutatif un groupe $\hat{W}(k)$ qui vérifie la propriété universelle suivante : tout morphisme de monoïdes de $\hat{W}_{\mathrm{mon}}(k)$ vers un groupe abélien G se factorise de façon unique par $\hat{W}(k)$. Concrêtement, il est construit comme $\mathbb{Z}$ à partir de $\mathbb{N}$ en prenant des différences formelles $q_1 - q_2$ d'éléments de $\hat{W}_{\mathrm{mon}}(k)$ et en quotientant par la bonne relation d'équivalence. Ici, puisque $\hat{W}_{\mathrm{mon}}(k)$ est un monoïde *simplifiable* par le théorème d'annulation de Witt (au sens où $x+y=x+z \implies y=z$), la relation d'équivalence par laquelle quotienter est simplement :

$$q_1 - q_2 \sim q_1' - q_2' \iff q_1 + q_2' = q_1' + q_2$$

et on a un morphisme *injectif* canonique :

$$\hat{W}_{\text{mon}}(k) \subseteq \hat{W}(k).$$

Ce dernier groupe s'appelle le groupe de *Grothendieck-Witt* de k et il est muni d'une structure d'anneau qui provient du produit tensoriel, dont l'élément neutre est $\langle 1 \rangle$. On a un morphisme d'anneau surjectif :

$$\hat{W}(k) \longrightarrow \mathbb{Z}$$

donné par la dimension et son noyau est *l'idéal fondamental* $\hat{I}$ de k. L'anneau $\hat{W}(k)$ dispose d'un élément en particulier appelé le plan hyperbolique :

$$\mathbb{H} = \langle 1, -1 \rangle$$

qui est l'unique forme quadratique de dimension 2 non dégénérée et isotrope à isomorphisme près.

Lemme 4.5.0.1. *Le sous-groupe engendré par* $\mathbb{H}$ *dans* $\hat{W}(k)$ *est un idéal de l'anneau* $\hat{W}(k)$.

Démonstration. Il s'agit de montrer que pour toute forme quadratique non-dégénérée q, la forme quadratique $q \otimes \langle 1, -1 \rangle$ est hyperbolique, c'est à dire est somme directe de plans hyperboliques. Notons $q = \langle a_1, \ldots, a_n \rangle$ de sorte que $q \otimes \mathbb{H} = \langle a_1, -a_1, \ldots, a_n, -a_n \rangle = n \cdot \mathbb{H}$ car pour tout $a \in k^\times$ la forme non-dégénérée $\langle a, -a \rangle$ est de dimension 2 et isotrope donc isomorphe à $\mathbb{H}$. □

Définition 4.5.0.2. *On définit l'anneau de Witt de k comme le quotient de* $\hat{W}(k)$ *par l'idéal (ou le sous-groupe) engendré par* $\mathbb{H}$. *On le note* $W(k)$ *et dans cet anneau, on a* $\langle 1 \rangle + \langle -1 \rangle = 0$ *autrement dit* $\langle -1 \rangle = -\langle 1 \rangle$. *Le morphisme de dimension défini précedemment induit un morphisme d'anneaux :*

$$W(k) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

qui donne la parité de la dimension. Son noyau I est encore appelé idéal fondamental.

Il est facile de vérifier que $W(k)$ est en bijection avec les formes anisotropes à isomorphisme près.

Définition 4.5.0.3. *Soit* ℓ/k *une extension de corps de caractéristique différente de* 2. *À toute forme quadratique q sur k on peut associer une forme quadratique* q_ℓ *sur* ℓ *par extension des scalaires. Si q est non-dégénérée,* q_ℓ *aussi car son discriminant dans une base reste inchangé après extension des scalaires. Il est alors clair qu'on obtient un morphisme d'anneaux :*

$$\hat{W}(k) \longrightarrow \hat{W}(\ell)$$

d'extension des scalaires. On note de plus que le plan hyperbolique est envoyé sur le plan hyperbolique par ce morphisme et donc on obtient un morphisme au niveau des anneaux de Witt également :

$$W(k) \longrightarrow W(\ell).$$

L'extension ℓ/k *est dite anisotrope si toute forme quadratique anisotrope sur k reste anisotrope sur* ℓ.

Remarque 4.5.0.4. Si ℓ/k est une extension anisotrope, alors $W(k) \longrightarrow W(\ell)$ est injectif, mais la réciproque n'a pas lieu d'être.

Le théorème suivant donne des exemples courants d'extensions anisotropes. Le second point est dû à *Springer*.

Théorème 4.5.0.5. *Toute extension purement transcendante est anisotrope. Toute extension finie de degré impair est anisotrope.*

Démonstration. Commençons par le premier point. On se donne $\ell = k(X_i \mid i \in I)$ une extension purement transcendante de k et q une forme quadratique anisotrope sur k. On suppose que q a un zéro non-trivial dans ℓ. Un tel zéro a alors ses coordonnées dans une sous-extension purement transcendante de type fini. Notons de plus que si L/K et M/L sont anisotropes, alors M/K est anisotrope. On se ramène donc par récurrence immédiate au cas où $\ell = k(X)$. Si q a un zéro non trivial dans ℓ, on a :

$$q(f_1, \ldots, f_m) = 0$$

et on peut supposer $f_i \in k[X]$ premiers entre eux dans leur ensemble par homogénéité de q. On évalue alors cette relation en $X = 0$ et on trouve un zéro non-trivial de q (par hypothèse les f_i ne s'annulent pas tous en 0).
Supposons maintenant que ℓ/k est une extension finie impaire de degré d. Par dévissage, on peut supposer que $\ell = k[x]$ avec P le polynôme minimal de x sur k de degré d. Soit q anisotrope sur k et soit $(y_1, \ldots, y_m)$ un zéro non-trivial de q dans ℓ. On peut écrire :

$$y_i = g_i(x)$$

avec $g_i \in k[T]$ de degré $d_i < d$. Par homogénéité de q, tant que les g_i ont des facteurs en commun, on peut les retirer (ce qui fait baisser leur degré) et donc on peut supposer, en plus de $d_i < d$, que les g_i sont premiers entre eux dans leur ensemble. On a alors :

$$q(g_1(T), \ldots, g_m(T)) = h(T)P(T)$$

dans $k[T]$ avec h un certain polynôme. Comme q est *anisotrope* sur k, le membre de gauche est de degré $2M$ avec M le maximum des d_i (si c'était de degré moindre, on obtiendrait un zéro non-trivial de q dans k). On obtient :

$$d + \deg(h) = 2M$$

donc $\deg(h)$ est *impair* et $\deg(h) \leq 2(d-1) - d = d - 2$. Comme h est non-constant, il possède une racine $\theta \in \overline{k}$ et on obtient, en évaluant en θ :

$$q(g_1(\theta), \ldots, g_m(\theta)) = 0$$

dans le corps $k[\theta]$ qui est toujours de degré impair mais strictement inférieur à d. Comme les g_i sont premiers entre eux dans leur ensemble, on a que q est isotrope sur ce corps et on conclut alors en faisant une récurrence sur d. □

4.6 Formes de Pfister

On se convainc facilement que l'idéal fondamental I de $W(k)$ défini dans la partie précédente est engendré par les formes $\langle 1, -a \rangle$ avec a qui n'est pas un carré (sinon cette forme est nulle). On note alors $\langle\langle a \rangle\rangle$ la forme $\langle 1, -a \rangle$ et plus généralement :

$$\langle\langle a_1, \ldots, a_n \rangle\rangle = \langle\langle a_1 \rangle\rangle \otimes \cdots \otimes \langle\langle a_n \rangle\rangle$$

et ce sont les formes qui génèrent I^n : on les appelle formes de Pfister. Ces formes ont des propriétés intéressantes, on montre notamment que si une forme de Pfister φ est isotrope, alors elle est hyperbolique (i.e. $\varphi = 0$ dans $W(k)$) et que l'ensemble des valeurs non-nulles de φ, noté $D(\varphi)$, est un sous-groupe de $k^\times$ (voir [16] théorèmes 1.6 et 1.7).

Lemme 4.6.0.1. *Soient $a_1, \dots, a_n \in k^\times$. Si l'un des a_i est un carré, ou bien si $a_i + a_j = 1$ pour $i \neq j$, alors on a :*

$$\langle\langle a_1, \dots, a_n \rangle\rangle = 0$$

dans $W(k)$. De plus, on a un morphisme d'anneaux gradués bien défini :

$$\mathrm{pf} : K_*(k)/(2) \longrightarrow \bigoplus_{n \geq 0} I^n/I^{n+1}.$$

qui à $\{a_1, \dots, a_n\}$ associe $\langle\langle a_1, \dots, a_n \rangle\rangle$.

Démonstration. Si $a \in k^\times$ est un carré, alors $\langle\langle a \rangle\rangle = \langle 1, -a \rangle = \langle 1, -1 \rangle = 0$ dans $W(k)$ et en prenant des produits on en déduit que si l'un des a_i est un carré la forme de Pfister s'annule dans $W(k)$. Ensuite, si $a + b = 1$ avec $a, b \in k^\times$, alors :

$$\langle\langle a, b \rangle\rangle = \langle 1, -a \rangle \langle 1, -b \rangle = \langle 1, -a, -b, ab \rangle = \left\langle 1, -a, a-1, a-a^2 \right\rangle$$

et cette forme prend la valeur -1 en l'appliquant au vecteur $(0, 1, 1, 0)$ et aussi la valeur 1 donc elle contient un plan hyperbolique et une forme de Pfister isotrope est nulle dans $W(k)$.
Ensuite, on observe, pour $a, b \in k^\times$:

$$\langle\langle ab \rangle\rangle = \langle 1, -ab \rangle = \langle\langle a \rangle\rangle + \langle\langle b \rangle\rangle - \langle\langle a, b \rangle\rangle$$

de sorte qu'on a un morphisme bien défini :

$$k^\times \longrightarrow I/I^2.$$

En passant à l'algèbre tensorielle on obtient un morphisme d'anneaux gradués :

$$T(k^\times) \longrightarrow T(I/I^2) \longrightarrow \bigoplus_{n \geq 0} I^n/I^{n+1}$$

et par la relation démontrée avant on a donc un morphisme depuis la K-théorie de Milnor. Comme les carrés sont tués par ce morphisme on a bien un morphisme comme annoncé. □

Puisque I^n est engendré par les formes de Pfister, ce morphisme pf est surjectif. En fait, Orlov, Vishik, et Voevodsky ont démontré en 1997 dans [29] en utilisant des techniques de cohomologie motivique que pf est un isomorphisme pour un corps de caractéristique différente de 2, ce qui constituait auparavant une conjecture de Milnor.

Théorème 4.6.0.2. *(Orlov-Vishik-Voevodsky) Soit k un corps de caractéristique différente de 2. Le morphisme :*

$$\mathrm{pf} : K_*(k)/(2) \longrightarrow \bigoplus_{n \geq 0} I^n/I^{n+1}$$

défini précedemment est un isomorphisme.

Certains cas particuliers sont faciles à traiter : en degré 0 les deux membres sont $\mathbb{Z}/2\mathbb{Z}$ et en degré 1 il s'agit de voir que :

$$k^\times/(k^\times)^2 \cong I/I^2$$

via le morphisme $x \mapsto \langle\langle x \rangle\rangle$. Pour cela on peut explicitement construire le morphisme réciproque, en envoyant la classe d'une forme non-dégénérée q sur :

$$(-1)^{\frac{n(n-1)}{2}} \operatorname{Disc} q$$

avec $n = \dim(q)$.

4.7 Symbole de Galois et conjecture de Bloch-Kato

Soit k un corps et $m \geq 1$ un entier premier à la caractéristique de k. On note encore G le groupe de Galois absolu de k. La théorie de Kummer donne un morphisme surjectif :

$$\nabla : k^\times \longrightarrow H^1(G, \mu_m)$$

dont le noyau est $(k^\times)^m$. En tensorisant n fois avec $n \geq 0$ et en appliquant le cup-produit, on obtient un morphisme :

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

appelé *n-ème symbole de Galois* et qui envoie $x_1 \otimes \cdots \otimes x_n$ sur $(\nabla x_1) \cup \cdots \cup (\nabla x_n)$ que l'on notera $h_n(x_1, \ldots, x_n)$. On observe d'ailleurs que si $\mu_m \subseteq k$, alors $\mu_m^{\otimes n} \cong \mu_m$ de façon non-canonique (il faut choisir un générateur).

Lemme 4.7.0.1. *Le symbole de Galois se factorise par la K-théorie de k, on a donc un morphisme de groupes :*

$$h_n : K_n(k) \longrightarrow H^n(G, \mu_m^{\otimes n}).$$

Plus précisément, on a un morphisme d'anneaux gradués :

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

où la structure d'anneau à droite est donnée par le cup-produit.

Démonstration. Il s'agit de vérifier que si $a + b = 1$ avec $a, b \in k^\times$, alors :

$$(\nabla a) \cup (\nabla b) = 0$$

dans $H^2(G, \mu_m^{\otimes 2})$. On factorise $X^m - a$ dans $k[X]$:

$$X^m - a = \prod_{i=1}^{r} f_i$$

avec f_i irréductible unitaire sur k. Chaque f_i possède une racine α_i et on pose $\ell_i = k[\alpha_i] \subseteq k_s$. En évaluant en 1 on obtient :

$$b = \prod_{i=1}^{r} f_i(1) = \prod_{i=1}^{r} N_{\ell_i/k}(1 - \alpha_i).$$

On a donc :

$$h_2(a, b) = \sum_{i=1}^{r} (\nabla a) \cup \Big(\nabla N_{\ell_i/k}(1 - \alpha_i) \Big).$$

On utilise ensuite le diagramme commutatif suivant :

$$\begin{array}{ccc}
\ell_i^\times & \xrightarrow{N_{\ell_i/k}} & k^\times \\
\| & & \| \\
H^0(G_{\ell_i}, k_s^\times) & \xrightarrow{\text{Cor}} & H^0(G_k, k_s^\times) \\
{\scriptstyle\nabla}\downarrow & & \downarrow{\scriptstyle\nabla} \\
H^1(G_{\ell_i}, \mu_m) & \xrightarrow{\text{Cor}} & H^1(G_k, \mu_m)
\end{array}$$

de sorte que :

$$h_2(a,b) = \sum_i (\nabla a) \cup \mathrm{Cor}^G_{G_{\ell_i}}(\nabla(1-\alpha_i)) = \sum_i \mathrm{Cor}^G_{G_{\ell_i}}\left(\mathrm{Res}^G_{G_{\ell_i}}(\nabla a) \cup \nabla(1-\alpha_i)\right)$$

et on note alors que $\mathrm{Res}^G_{G_{\ell_i}}(\nabla a) = \nabla_{\ell_i}(a) = \nabla_{\ell_i}(\alpha_i^m) = 0$ car ∇ tue $(\ell_i^\times)^m$. Ainsi :

$$h_2(a,b) = 0$$

comme voulu. □

Puisque $(k^\times)^m$ est tué par ∇, on a même un morphisme d'anneaux gradués :

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

dont on remarque que c'est un isomorphisme en degrés 0 et 1.

Théorème 4.7.0.2. *La conjecture de Bloch-Kato, démontrée par Voevodsky et Rost (voir [25]) et ainsi devenue le théorème d'isomosphisme de norme et résidu, affirme que :*

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

est un isomorphisme d'anneaux gradués.

Pour $n = 2$, on obtient notamment que le groupe de Brauer est engendré par les algèbres cycliques. De plus, cet isomorphisme fait aussi correspondre, d'une part les morphismes de norme en K-théorie, et d'autre part les morphismes de corestriction en cohomologie galoisienne.

Chapitre 5

Faisceaux cohérents et théorie de l'intersection

5.1 Groupe de Grothendieck des faisceaux cohérents

Pour la suite, nous aurons besoin de quelques notions et résultats géométriques. Commençons par définit le groupe de Grothendieck des faisceaux cohérents sur un schéma.

Définition 5.1.0.1. *Soit X un schéma. On considère le groupe abélien libre engendré par les classes d'isomorphisme de faisceaux cohérents sur X, quotienté par le sous-groupe engendré par les $[\mathcal{F}]+[\mathcal{H}]-[\mathcal{G}]$ pour chaque suite exacte $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$. On note ce groupe $K(X)$: c'est le groupe de Grothendieck des faisceaux cohérents sur X. De même, on définit $K^{\mathrm{lf}}(X)$, le groupe de Grothendieck des faisceaux localement libres de type fini sur X, qui est défini de la même manière en partant des classes d'isomorphisme de faisceaux localement libres de type fini sur X.*

Remarque 5.1.0.2. La définition précédente a du sens car on peut trouver un système de représentant des faisceaux cohérents à isomorphisme près qui soit un ensemble. En effet, pour chaque ouvert affine $\operatorname{Spec} A$ d'un recouvrement de X, les A-modules de présentation finie sur A sont des conoyaux de matrices finies.

Si X est un schéma propre sur un corps et $\mathcal{F}$ un faisceau cohérent sur X, la caractéristique d'Euler $\chi(X,\mathcal{F})$ ne dépend que de la classe de $\mathcal{F}$ dans le groupe $K(X)$ et on a alors un morphisme de groupes :

$$K(X) \xrightarrow{\chi} \mathbb{Z}.$$

Le groupe $K(X)$ se comporte bien vis-à-vis des dévissages (de la même façon que le groupe des classes).

Proposition 5.1.0.3. *Soit X un schéma, $Z \subseteq X$ un sous-schéma fermé et U le complémentaire de Z. On a une suite exacte :*

$$K(Z) \longrightarrow K(X) \longrightarrow K(U) \longrightarrow 0$$

où la première flèche s'obtient par poussé en avant et la deuxième par restriction à U.

On renvoie à l'article de Borel et Serre pour la preuve de cet énoncé [1]. Notons simplement que les deux flèches sont bien définies au niveau des groupes de Grothendieck car le poussé en avant par une immersion fermée et le tiré en arrière par une immersion ouverte sont exacts.

Proposition 5.1.0.4. *Soit X un schéma noéthérien. Le groupe $K(X)$ est engendré par les $[i_*\mathcal{O}_Z]$ avec $Z \xrightarrow{i} X$ un fermé intègre de X.*

Démonstration. On raisonne par récurrence sur la dimension et le nombre de composantes irréductibles de X. Si X est vide, c'est clair. Si X est irréductible, on peut aussi le supposer intègre car $K(X)$ est un quotient de $K(X^{\mathrm{red}})$ d'après la suite exacte 5.1.0.3. Soit alors $\mathcal{F}$ un faisceau cohérent sur X. Il existe un ouvert non-trivial U sur lequel $\mathcal{F}$ est localement libre. Notons Z le complémentaire réduit de U, i l'immersion fermée de Z et j l'immersion ouverte de U. On a une suite exacte :

$$0 \longrightarrow \mathcal{K} \longrightarrow \mathcal{F} \longrightarrow j_*\mathcal{F}_{|U} \longrightarrow \mathcal{C} \longrightarrow 0$$

avec $\mathcal{K}$ et $\mathcal{C}$ supportés sur Z. Puisque Z est de dimension strictement plus petite que celle de X, on se ramène donc au cas de $j_*\mathcal{F}_{|U}$ qui est localement libre, donc libre quitte à restreindre U. On se ramène donc à montrer que la classe de $j_*\mathcal{O}_U$ est bien engendrée par les classes annoncées. Pour cela on considère le morphisme $\mathcal{O}_X \longrightarrow j_*\mathcal{O}_U$ dont le noyau et conoyau sont supportés sur Z ce qui réduit entièrement le problème à la question du faisceau $\mathcal{O}_X$. Or X est intègre donc $\mathcal{O}_X$ est bien de la forme souhaitée.
Supposons à présent que X possède au moins 2 composantes irréductibles.
Si Z est une composante irréductible (réduite) de X et si $\mathcal{F}$ est un faisceau sur X, on a un morphisme :

$$\mathcal{F} \longrightarrow j_*\mathcal{F}_{|U}$$

avec $j : U \longrightarrow X$ l'immersion ouverte du complémentaire de Z. C'est un isomorphisme en tout point de U donc le noyau et conoyau sont supportés sur Z, et puisque Z est intègre, on connaît l'énoncé pour Z donc on se ramène au cas de $j_*\mathcal{F}_{|U}$. Puisque U possède une composante irréductible de moins, par récurrence on peut écrire $[\mathcal{F}_{|U}]$ comme combinaison linéaire de faisceaux $\iota_{\lambda,*}\mathcal{O}_{T_\lambda \cap U}$ avec T_λ fermé intègre de X. Comme d'habitude, on considère alors le morphisme :

$$(T_\lambda \longrightarrow X)_*\mathcal{O}_{T_\lambda} \longrightarrow (T_\lambda \cap U \longrightarrow X)_*\mathcal{O}_{T_\lambda \cap U}$$

qui est un isomorphisme en tout point de U et dont le noyau et conoyau sont donc supportés sur Z, ce qui permet de conclure. □

5.2 Principe de dévissage de Wittenberg et indices de variétés propres

Dans la suite, on note $\chi(X,\mathcal{F})$ la caractéristique d'Euler d'un faisceau cohérent sur un k-schéma propre X et $\chi(X)$ la caractéristique d'Euler de X, définie comme $\chi(X,\mathcal{O}_X)$. On définit alors les trois notions d'indices suivantes.

Définition 5.2.0.1. *(Indices d'une variété propre sur un corps)*
Soit k un corps et X un k-schéma propre. On définit :

- *L'indice de X sur k, noté $[X : k]$, comme le* pgcd *des degrés des extensions finies ℓ/k avec $X(\ell) \neq \emptyset$.*
- *L'indice étendu de X sur k, noté $[X : k]_{\text{ét}}$, comme le* pgcd *des degrés des extensions k_Z/k, clôture algébrique de k dans $k(Z)$ pour Z fermé intègre de X (ce sont des extensions finies car $k(Z)$ est une extension de type fini de k).*
- *L'indice cohomologique de X sur k, noté $[X : k]_\chi$ comme le* pgcd *des caractéristiques d'Euler-Poincaré des faisceaux cohérents sur X.*

En spécialisant aux faisceaux cohérents $j_*\mathrm{Spec}\,k(P)$ pour P un point fermé de X et $j : \mathrm{Spec}\,k(P) \longrightarrow X$, on obtient une première relation de divisibilité :

$$[X : k]_\chi \mid [X : k].$$

Notons que si X est géométriquement intègre, alors $[X : k]_{\text{ét}} = 1$.

La proposition 5.1.0.4 permet de démontrer le principe de dévissage suivant dû à Wittenberg dans [30].

Théorème 5.2.0.2. *(Principe de dévissage de Wittenberg)*
Soit k un corps, $D \geq 0$ un entier, et, pour chaque k-schéma propre de dimension au plus D (à isomorphisme près), un entier $n_X \geq 1$.
On suppose que si $Y \longrightarrow X$ est un morphisme de k-schémas propres de dimension au plus D, on a $n_X \mid n_Y$ et que pour tout k-schéma propre intègre X de dimension au plus D, il existe $f : Y \longrightarrow X$ dominante avec Y/k propre et intègre, n_X et $\chi(Y_\eta)$ premiers entre eux, en notant Y_η la fibre générique, et $n_Y \mid \chi(Y)$.
Alors pour tout k-schéma propre X de dimension au plus D, et pour tout faisceau cohérent $\mathcal{F}$ sur X, on a :

$$n_X \mid \chi(X, \mathcal{F}).$$

Démonstration. D'après la proposition 5.1.0.4, et comme la caractéristique d'Euler est additive, on peut supposer que $\mathcal{F}$ est le faisceau des fonctions sur un fermé intègre Z de X, et comme $n_X \mid n_Z$ et comme $\chi(X, \mathcal{F}) = \chi(Z)$, on peut supposer que X est intègre et qu'on s'intéresse au faisceau $\mathcal{F} = \mathcal{O}_X$. On veut donc voir que $n_X \mid \chi(X)$.
On se donne alors un $f : Y \longrightarrow X$ dominant comme dans l'énoncé, avec Y/k propre intègre. Comme X est de dimension finie, les $R^q f_*\mathcal{O}_Y$ sont nuls à partir d'un certain rang et il existe donc un ouvert dense U tel que $(R^q f_*\mathcal{O}_Y)_{|U}$ soit libre pour tout q. On a alors l'égalité suivante dans le groupe $K(U)$:

$$\sum_q (-1)^q [R^q f_*\mathcal{O}_Y]_{|U} = \left(\sum_q (-1)^q r(q)\right)[\mathcal{O}_U]$$

avec $r(q)$ le rang de $R^q f_*\mathcal{O}_Y$. Notons alors que, si η désigne le point générique de X et Y_η est la fibre générique, on a :

$$H^q(Y_\eta, \mathcal{O}_{Y_\eta}) = \mathrm{colim}_V\, H^q(f^{-1}(V), \mathcal{O}_Y) = (R^q f_*\mathcal{O}_Y)_\eta = (\mathcal{O}_X)_\eta^{r(q)}$$

donc :

$$\chi(Y_\eta) = \sum_q (-1)^q r(q).$$

Ainsi :

$$\chi(Y_\eta)[\mathcal{O}_U] = \sum_q (-1)^q [R^q f_*\mathcal{O}_Y]_{|U}$$

et donc par la suite exacte pour le groupe de Grothendieck 5.1.0.3, il existe $\alpha \in K(Z)$ avec $Z = X \setminus U$ tel que :

$$\chi(Y_\eta)[\mathcal{O}_X] = \sum_q (-1)^q [R^q f_*\mathcal{O}_Y] + i_*\alpha.$$

Or on a une suite spectrale :

$$H^q(X, R^p f_*\mathcal{O}_Y) \implies H^{p+q}(Y, \mathcal{O}_Y)$$

et on note E_2 la deuxième page. On définit la caractéristique d'Euler d'une page $E_r^{\bullet,\bullet}$ comme $\sum_{p,q}(-1)^{p+q}\dim E_r^{p,q}$ et il est facile de vérifier que la caractéristique d'Euler ne change pas lorsqu'on tourne une page dans la suite spectrale. On a donc $\chi(E_2)=\chi(E_\infty)=\chi(Y)$.
On obtient donc :

$$\chi(Y_\eta)\chi(X)=\chi(Y)+\chi(Z,\alpha).$$

Comme n_X est premier avec $\chi(Y_\eta)$, et comme $n_X \mid n_Y \mid \chi(Y)$ et $n_X \mid n_Z \mid \chi(Z,\alpha)$ en appliquant une récurrence noéthérienne à Z, on conclut. □

Dans bien des situations, on aura même f génériquement finie, ce qui, sur un corps parfait, entraîne que la quantité $\chi(Y_\eta)$ est égale au *degré* (générique) de f car f est génériquement étale donc $\chi(Y_\eta)=\chi(Y_p)$ pour presque tout point fermé p de X, et Y_p est une somme directe de $\deg(f)$ copies de $\operatorname{Spec} k(p)$.
De ce principe de dévissage, on obtient le corollaire suivant.

Corollaire 5.2.0.3. *(L'indice étendu divise l'indice cohomologique)*
Soit k un corps parfait, X un k-schéma propre et $\mathcal{F}$ un faisceau cohérent sur X. On a alors :

$$[X:k]_{\text{ét}} \mid [X:k]_\chi \mid [X:k].$$

Démonstration. On applique le théorème de dévissage 5.2.0.2 : si $f : Y \longrightarrow X$ est un morphisme de k-schémas propres, alors on a :

$$[X:k]_{\text{ét}} \mid [Y:k]_{\text{ét}}$$

car pour tout fermé intègre Z de Y, $f(Z)^{\text{red}}$ est un fermé intègre de X et on a un morphisme $k_{f(Z)} \longrightarrow k_Z$ au dessus de k.
Ensuite, si X est un schéma propre intègre sur k, on peut considérer sa normalisation $\widetilde{X} \longrightarrow X$ qui est encore un k-schéma propre et intègre. Le morphisme de normalisation est birationnel donc la condition de primalité est bien respectée, et $\mathcal{O}_{\widetilde{X}}$ est un faisceau en $k_{\widetilde{X}}$-espaces vectoriels car $\widetilde{X}$ est normal donc on peut voir $\widetilde{X}$ comme un k_X-schéma qu'on note $\widetilde{X}'$, de sorte que :

$$\chi(\widetilde{X})=\sum_i(-1)^i\dim_k H^i(\widetilde{X},\mathcal{O}_{\widetilde{X}})=\sum_i(-1)^i[k_{\widetilde{X}}:k]\dim_{k_{\widetilde{X}}}H^i(\widetilde{X},\mathcal{O}_{\widetilde{X}})=[k_{\widetilde{X}}:k]\chi(\widetilde{X}')$$

et ainsi $[\widetilde{X}:k_X]_{\text{ét}} \mid \chi(\widetilde{X})$. □

5.3 Théorie de l'intersection sur un schéma de type fini sur un corps

Soit X un schéma de type fini sur un corps K. On considère, pour tout $k \geq 0$, le groupe $Z_k(X)$ des combinaisons formelles de sous-schémas fermés intègres de dimension k de X, appelés *cycles de dimension k*. Pour tout morphisme propre $f : X \longrightarrow Y$ de schémas noéthériens sur K, on dispose d'un poussé en avant $f_* : Z_k(X) \longrightarrow Z_k(Y)$ défini de la façon suivante : si Z est un fermé intègre de X, ou bien $\dim f(Z) < \dim Z$ et on pose $f_*[Z]=0$, ou bien $\dim f(Z)=\dim Z$ auquel cas on pose :

$$f_*[Z]=\deg(f_{|Z})[f(Z)].$$

Ici, il faut comprendre $f_{|Z} : Z \longrightarrow f(Z)$ avec sur $f(Z)$ la structure réduite. Le degré est fini car $K(Z)/K(f(Z))$ est de type fini et les deux corps ont même degré de transcendance sur K.

Si f est une immersion fermée, on a simplement $f_*[Z] = [Z]$.
On rappelle aussi que si X est intègre de corps des fractions $K(X)$, il est possible d'associer à toute fraction rationnelle $f \in K(X)^\times$ un diviseur de Weil de la façon suivante. Pour chaque fermé intègre Z de codimension 1 de X, l'anneau $\mathcal{O}_{X,Z}$ est défini comme l'anneau local en un point générique de Z, et c'est un anneau intègre local de dimension 1. Ainsi, si $f \in \mathcal{O}_{X,Z} \setminus \{0\}$, la quantité :

$$v_Z(f) = \mathrm{len}_{\mathcal{O}_{X,Z}}(\mathcal{O}_{X,Z}/(f))$$

est bien définie car $\mathcal{O}_{X,Z}/(f)$ est noéthérien de dimension 0 donc Artinien, et il est facile de voir qu'elle s'étend en un morphisme de groupes $v_Z : K(X)^\times \longrightarrow \mathbb{Z}$, en considérant, pour $f, g \in \mathcal{O}_{X,Z} \setminus \{0\}$, la suite exacte :

$$0 \longrightarrow O_{X,Z}/(g) \xrightarrow{\bullet \times f} O_{X,Z}/(fg) \longrightarrow O_{X,Z}/(f) \longrightarrow 0.$$

On définit alors le *diviseur* de f par la formule suivante :

$$\mathrm{div}(f) = \sum_Z v_Z(f)[Z] \in Z_{d-1}(X)$$

avec la somme qui porte sur les fermés intègres de codimension 1 (seul un nombre fini d'entre eux donne une valuation non-nulle).
Si $\mathcal{O}_{X,Z}$ est normal (ou de façon équivalente, régulier), alors c'est un anneau de valuation discrète et $v_Z(f)$ est simplement la valuation de f dans cet anneau.
On peut alors définit les groupes de Chow d'un schéma de type fini sur K.

Définition 5.3.0.1. *(Groupes de Chow) Soit X un schéma de type fini sur un corps K.*
Un cycle $C \in Z_k(X)$ est rationnellement équivalent à 0 s'il existe des fermés intègres de dimension $k+1$, $Z_i \xrightarrow{j_i} X$ et des fonctions rationnelles non-nulles f_i sur Z_i telles que :

$$C = \sum_i j_{i,*}\,\mathrm{div}(f_i).$$

On définit alors le groupe de Chow de dimension k de X comme le quotient du groupe $Z_k(X)$ par le groupe des cycles rationnellement équivalents à 0, et on le note $\mathrm{Chow}_k(X)$.

Bien souvent, il est plus avantageux d'utiliser la numérotation par la *codimension* comme on le verra dans la suite : si X est irréductible de dimension d ou si toutes les composantes irréductibles de X ont dimension d, on peut définir $\mathrm{Chow}^k(X) = \mathrm{Chow}_{d-k}(X)$. On définit de même $Z^k(X) = Z_{d-k}(X)$.
Ainsi, $\mathrm{Chow}^d(X)$ est le groupe des 0-cycles de X à équivalence rationnelle près, et $\mathrm{Chow}^1(X)$ s'identifie au groupe des classes de diviseurs de Weil, $\mathrm{Cl}(X)$.
On note enfin :

$$\mathrm{Chow}(X) = \bigoplus_k \mathrm{Chow}^k(X).$$

Si $f : X \longrightarrow Y$ est un morphisme propre de K-schémas de type fini, les morphismes $f_* : Z_k(X) \longrightarrow Z_k(Y)$ définis plus haut induisent un morphisme gradué de *poussé en avant* :

$$f_* : \mathrm{Chow}(X) \longrightarrow \mathrm{Chow}(Y).$$

Remarque 5.3.0.2. Si X est propre sur K, le morphisme $X \longrightarrow \mathrm{Spec}(K)$ induit un morphisme $\mathrm{Chow}_0(X) \longrightarrow \mathrm{Chow}_0(\mathrm{Spec}\,K) = \mathbb{Z}$. Il est facile de vérifier que ce morphisme est donné par le degré d'un 0-cycle.

Donnons les groupes de Chow des variétés de base.

Proposition 5.3.0.3. *On a* $\mathrm{Chow}(\mathbb{A}^n_K) = \mathbb{Z}[\mathbb{A}^n]$ *et* $\mathrm{Chow}^k(\mathbb{P}^n_K) = \mathbb{Z}$ *pour* $0 \leq k \leq n$.

Remarque 5.3.0.4. Les outils utilisés pour faire ces calculs consistent en la suite exacte d'excision pour les groupes de Chow et la méthode de stratification par des schémas affines. On renvoie à [3], section 1.2, pour les détails.

Si X est un schéma projectif lisse et intègre sur K, on peut munir $\mathrm{Chow}(X)$ d'une structure d'anneau gradué.

Définition 5.3.0.5. *Soient* Z_1, Z_2 *deux fermés intègres de* X *de dimensions* r *et* s. *On dit que* Z_1 *et* Z_2 *s'intersectent proprement si* $\dim(Z_1 \cap Z_2) \leq r + s - \dim(X)$, *ou de façon équivalente, en notant* k, ℓ *les codimensions de* Z_1 *et* Z_2 *:*

$$\mathrm{codim}(Z_1 \cap Z_2) \geq k + \ell.$$

Si $\alpha = \sum_i \lambda_i Z_i \in Z^k(X)$ *et* $\beta = \sum_j \mu_j W_j \in Z^\ell(X)$, *on dit que* α *et* β *s'intersectent proprement si les* Z_i *intersectent proprement les* W_j *dès que* $\lambda_i \neq 0$ *et* $\mu_j \neq 0$. *On définit alors l'intersection de* α *et* β *via la formule suivante :*

$$\alpha \cap \beta = \sum_{i,j} \lambda_i \mu_j [Z_i \cap W_j] \in Z^{k+\ell}(X)$$

où $[Z_i \cap W_j] = 0$ *si* $Z_i \cap W_j$ *est vide (ou de façon équivalente, si il est de codimension strictement plus grande que* $k + \ell$*).*

La construction de la structure d'anneau sur le groupe de Chow repose alors sur le lemme suivant, dit *moving lemma*.

Lemme 5.3.0.6. *Soit* X *un schéma projectif lisse intègre sur* K, $\alpha \in Z^k(X)$ *et* $\beta \in Z^\ell(X)$. *Il existe alors* α' *égal à* α *dans le groupe de Chow, tel que* α' *et* β *s'intersectent proprement.*
De plus, si α *et* β *s'intersectent proprement et si* $[\alpha] = 0$ *dans le groupe de Chow, alors* $[\alpha \cap \beta] = 0$ *dans le groupe de Chow également.*

C'est alors une conséquence immédiate de ce lemme qu'il existe une unique structure d'anneau gradué commutatif sur $\mathrm{Chow}(X)$ tel que, si $[\alpha] \in \mathrm{Chow}^k(X), [\beta] \in \mathrm{Chow}^\ell(X)$ avec α et β qui *s'intersectent proprement*, on a :

$$[\alpha][\beta] = [\alpha \cap \beta].$$

Notons que l'élément neutre de l'anneau de Chow est toujours donné par la classe $[X]$.
Il est aussi possible de définir une structure de produit sur l'anneau de Chow d'une variété quasi-projective lisse intègre sur K.
On peut alors décrire la structure d'anneau de $\mathrm{Chow}(\mathbb{P}^n)$:

$$\mathrm{Chow}(\mathbb{P}^n) = \mathbb{Z}[\zeta]/(\zeta^{n+1})$$

avec ζ la classe d'un hyperplan quelconque.
Notons de plus que si Z est un fermé intègre de $\mathbb{P}^n$ de dimension k, on peut lui associer sa classe dans $\mathrm{Chow}_k(\mathbb{P}^n) = \mathbb{Z}$ qui est le *degré* de Z. C'est un entier positif, que l'on peut aussi définir via le polynôme de Hilbert de Z.

5.4 Classes de Chern et formule de Riemann-Roch-Hirzebruch

Soit X un schéma intègre de type fini lisse sur un corps K. À tout fibré en droites $\mathcal{L}$ sur X, on peut associer une classe de diviseurs $[\mathrm{div}(\mathcal{L})] \in \mathrm{Cl}(\mathcal{L})$ qui est un élément du groupe des classes de diviseurs de Weil de X, de la façon suivante : on choisit s une section rationnelle de $\mathcal{L}$, et pour chaque Z fermé intègre de codimension 1, on fixe une trivialisation locale de $\mathcal{L}$ autour de Z, ce qui donne un isomorphisme de $\mathcal{O}_{X,Z}$-modules :

$$\varphi : \mathcal{L}_Z \longrightarrow \mathcal{O}_{X,Z}$$

qui, en tensorisant par $K(X)$ permet d'envoyer s sur un élément $\varphi_*(s) \in \mathcal{O}_{X,Z}$ dont la valuation en Z est indépendante du choix de la trivialisation, on la note donc naturellement $v_Z(s)$. On peut donc poser :

$$\mathrm{div}(s) = \sum_Z v_Z(s)[Z]$$

et remarquer que la classe de ce diviseur ne dépend que de la classe d'isomorphisme de $\mathcal{L}$ à cause de la formule $\mathrm{div}(fs) = \mathrm{div}(f) + \mathrm{div}(s)$. Il est alors facile de voir qu'on a ainsi construit un morphisme de groupes :

$$\mathrm{Pic}(X) \longrightarrow \mathrm{Cl}(X)$$

et le groupe $\mathrm{Cl}(X)$ s'identifiant à $\mathrm{Chow}^1(X)$, on a un morphisme :

$$c_1 : \mathrm{Pic}(X) \longrightarrow \mathrm{Chow}^1(X).$$

Puisque X est régulier, c'est un isomorphisme. On souhaite étendre la définition de c_1 à tous les fibrés vectoriels sur X, et définir aussi d'autres applications c_n, appelées *classes de Chern*. De façon générale, on peut construire pour $\mathcal{F}$ un fibré vectoriel sur X, des classes $c_n(\mathcal{F}) \in \mathrm{Chow}^n(X)$ avec $c^0(\mathcal{F}) = 1$. On pose d'ailleurs pour plus de simplicité :

$$c(\mathcal{F}) = 1 + c_1(\mathcal{F}) + c_2(\mathcal{F}) + \cdots \in \mathrm{Chow}(X).$$

Ces classes de Chern vérifient les propriétés suivantes.

Proposition 5.4.0.1. *Pour toute suite exacte de fibrés vectoriels $0 \longrightarrow \mathcal{E} \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow 0$, on a :*

$$c(F) = c(E)c(G) \in \mathrm{Chow}(X).$$

De plus, les classes de Chern sont fonctorielles, au sens où si $f : Y \longrightarrow X$ est un morphisme entre deux variétés lisses quasi-projectives, on a :

$$f^* c(\mathcal{F}) = c(f^* \mathcal{F})$$

pour tout $\mathcal{F}$ fibré en droites sur Y (voir [3], 1.3.6 pour la définition du tiré en arrière sur le groupe de Chow).
Enfin, si $\mathcal{L}$ est un fibré en droites, on a simplement :

$$c(\mathcal{L}) = 1 + c_1(\mathcal{L}).$$

Puisque $1 - c(\mathcal{F})$ est nilpotent dans $\mathrm{Chow}(X)$, $c(\mathcal{F})$ est inversible et on a donc un morphisme de groupes bien défini :

$$K^{\mathrm{lf}}(X) \longrightarrow \mathrm{Chow}(X)^\times$$

du groupe de Grothendieck des fibrés vectoriels sur X vers le groupe des inversibles de l'anneau de Chow de X.

Dans notre cas, comme X est un schéma régulier, le groupe $K^{\mathrm{lf}}(X)$ s'identifie au groupe $K(X)$ de Grothendieck des faisceaux cohérents sur X (voir [1]) de sorte qu'on peut étendre la définition des classes de Chern à tout faisceau cohérent sur X tout en gardant ces propriétés.
Pour calculer les classes de Chern, la recette est la suivante : si $\mathcal{F} \cong \bigoplus_{i=1}^{k} \mathcal{L}_i$ est une somme de fibrés en droites, ou plus généralement si $\mathcal{F}$ admet une filtration dont le gradué est une somme de fibrés en droites $\mathcal{L}_i$, on a, par 5.4.0.1 :

$$c(\mathcal{F}) = \prod_i c(\mathcal{L}_i) = \prod_i (1 + c_1(\mathcal{L}_i))$$

Bien sûr, il n'est pas vrai que tout fibré vectoriel est somme directe de fibrés en droites, ni même se filtre avec des fibrés en droites. En général, on utilise le lemme suivant.

Lemme 5.4.0.2. *(Scindage d'un fibré en droite) Soit $\mathcal{F}$ un fibré vectoriel sur X. Il existe alors $f : Y \longrightarrow X$ plat, projectif, avec Y lisse et intègre, un morphisme de k-schémas, tel que le tiré en arrière* $\mathrm{Chow}(X) \longrightarrow \mathrm{Chow}(Y)$ *soit injectif et tel que $f^*\mathcal{F}$ admette une filtration par des fibrés vectoriels dont les quotients successifs sont des fibrés en droites.*

Ainsi, on peut tirer en arrière $\mathcal{F}$, calculer ses classes de Chern dans $\mathrm{Chow}(Y)$, qui seront des éléments de $\mathrm{Chow}(X)$ à cause de la fonctorialité des classes de Chern.
Si $f^*\mathcal{F}$ est filtré avec pour quotients successifs $\mathcal{L}_1, \ldots, \mathcal{L}_n$ des fibrés en droites, on appelle $\alpha_i = c_1(\mathcal{L}_i) \in \mathrm{Chow}(Y)$ les *racines de Chern* de $\mathcal{F}$. Ces éléments ne sont pas bien définis, mais tout polynôme symétrique appliqué en les α_i donne un élément bien défini de $\mathrm{Chow}(X)$ qui est un polynôme en les $c_j(\mathcal{F})$. En effet, on a :

$$1 + c_1(\mathcal{F}) + c_2(\mathcal{F}) + \cdots + c_d(\mathcal{F}) = \prod_i (1 + \alpha_i)$$

ce qui donne, en identifiant les termes dans la graduation :

$$c_i(\mathcal{F}) = \Sigma_i(\alpha_1, \ldots, \alpha_n)$$

avec Σ_i le i-ème polynôme symétrique élémentaire, or on a :

$$\mathbb{Z}[\alpha_1, \ldots, \alpha_n]^{\mathfrak{S}_n} = \mathbb{Z}[\Sigma_1, \ldots, \Sigma_n].$$

Cette observation permet de définir le caractère de Chern et la classe de Todd $\mathrm{Ch}(\mathcal{F})$ et $\mathrm{Td}(\mathcal{F})$:

$$\mathrm{Ch}(\mathcal{F}) = \sum_i \exp(\alpha_i) \in \mathrm{Chow}(X) \otimes \mathbb{Q}$$

et :

$$\mathrm{Td}(\mathcal{F}) = \prod_i Q(\alpha_i) \in \mathrm{Chow}(X) \otimes \mathbb{Q}$$

avec :

$$Q(x) = \frac{x}{1 - e^{-x}} = 1 + \frac{x}{2} + \sum_{k \geq 1} \frac{(-1)^{k-1} B_k}{(2k)!} x^{2k}.$$

Tout ceci est bien défini car les racines de Chern sont nilpotentes.
Dans la suite, on aura besoin d'un peu plus de précision arithmétique :

Proposition 5.4.0.3. *Si X est quasi-projectif, lisse, intègre, de dimension d sur K et $\mathcal{F}$ est un fibré en droites sur X, on peut définir* $\mathrm{Ch}(\mathcal{F})$ *et* $\mathrm{Td}(\mathcal{F})$ *plus précisément comme des éléments de* $\mathrm{Chow}(X)\otimes\mathbb{Z}\left[\frac{1}{d!}\right]$ *et* $\mathrm{Chow}(X)\otimes\mathbb{Z}\left[\frac{1}{(2d)!}\right]$ *respectivement.*

Démonstration. Notons $\alpha_1,\dots,\alpha_k$ "les" racines de Chern de $\mathcal{F}$, avec k le rang de $\mathcal{F}$.
On a un morphisme :

$$\mathbb{Z}[[t_1,\dots,t_k]]^{\mathfrak{S}_k}\longrightarrow \mathrm{Chow}(X)$$

défini par $t_i\mapsto\alpha_i\in\mathrm{Chow}(Y)$ en choisissant Y comme dans 5.4.0.2. Notons alors I l'idéal de $\mathbb{Z}[[t_1,\dots,t_k]]$ engendré par les monômes de degré strictement plus grand que d. Puisque $\mathrm{Chow}^i(X)=0$ pour $i>d$, on a un morphisme :

$$A=\mathbb{Z}[[t_1,\dots,t_k]]^{\mathfrak{S}_k}/I^{\mathfrak{S}_k}\longrightarrow \mathrm{Chow}(X).$$

Ainsi, si l'on considère les éléments $f=\sum_i\exp(t_i)$ et $g=\prod_i Q(t_i)$, leur image dans $A\otimes\mathbb{Q}$ tombe respectivement dans $A\otimes\mathbb{Z}[1/d!]$ et dans $A\otimes\mathbb{Z}[1/(2d)!]$ car, comme on le voit en calculant le développement en série entière de Q, on a :

$$Q(x)\in\mathbb{Z}[1/(2d)!][x]+(x^{d+1})\mathbb{Q}[[x]].$$

Ceci permet de conclure. □

On aura besoin du théorème de Riemann-Roch-Hirzebruch dans la suite. Pour cela, on adopte la notation suivante : le morphisme $\mathrm{Chow}(X)\longrightarrow\mathrm{Chow}(\mathrm{Spec}\,K)=\mathbb{Z}$ obtenu par poussé en avant sera noté $\int_X$ par analogie avec la géométrie complexe. Concrêtement, c'est le morphisme qui donne le degré de la partie 0-cycle d'un élément du groupe de Chow.

Théorème 5.4.0.4. *(Riemann-Roch-Hirzebruch)*
Soit X un schéma intègre projectif lisse sur un corps K et $\mathcal{F}$ un fibré en droites sur X. On a l'égalité suivante :

$$\chi(X,\mathcal{F})=\int_X \mathrm{Td}(\mathcal{T}_X)\,\mathrm{Ch}(\mathcal{F})\in\mathbb{Q}$$

avec $\mathcal{T}_X$ le fibré tangent de X.

Remarque 5.4.0.5. Notons que ceci entraîne directement le fameux théorème de Riemann-Roch pour les courbes. En effet, si X est une courbe projective lisse géométriquement intègre sur K et $\mathcal{L}$ un fibré en droites sur X, on a simplement :

$$\mathrm{Ch}(\mathcal{L})=1+c_1(\mathcal{L})$$

et :

$$\mathrm{Td}(\mathcal{T}_X)=1+\frac{1}{2}c_1(\mathcal{T}_X)=1-\frac{\mathcal{K}_X}{2}$$

avec $\mathcal{K}_X$ la classe du diviseur canonique. La formule de Riemann-Roch-Hirzebruch donne alors :

$$\chi(X,\mathcal{L})=\int_X\left(1+c_1(\mathcal{L})-\frac{\mathcal{K}_X}{2}\right)=\deg(\mathcal{L})-\frac{1}{2}\deg(\mathcal{K}_X).$$

Ceci se réécrit, grâce à la dualité de Serre, en notant D le diviseur associé à $\mathcal{L}$:

$$h^0(D)-h^0(\mathcal{K}_X-D)=\deg(D)-\frac{1}{2}\deg(\mathcal{K}_X).$$

En appliquant ceci au diviseur canonique, on obtient :

$$h^0(\mathcal{K}_X) - 1 = \frac{1}{2}\deg(\mathcal{K}_X)$$

dont on déduit $\deg(\mathcal{K}_X) = 2g(X) - 2$ avec $g(X) = h^0(\mathcal{K}_X)$ le genre de la courbe. On a donc bien :

$$h^0(D) - h^0(\mathcal{K}_X - D) = \deg(D) + 1 - g.$$

Du théorème de Riemann-Roch-Hirzebruch et de la considération arithmétique précédente, on déduit le corollaire suivant.

Corollaire 5.4.0.6. *Soit X un schéma projectif lisse intègre de dimension d sur un corps K et $\mathcal{F}$ un fibré vectoriel sur X. On a :*

$$[X : K]_\chi \in [X : K]\mathbb{Z}[1/(2d)!]$$

où l'on rappelle que $[X : K]$ est l'indice de X/K, défini comme le pgcd *des degrés des corps résiduels de X sur K, et $[X : K]_\chi$ est l'indice cohomologique de X sur K, défini en 5.2.0.1 comme le* pgcd *des caractéristiques d'Euler-Poincaré des faisceaux cohérents sur X.*

Démonstration. On a, pour tout faisceau cohérent $\mathcal{F}$ sur X :

$$\chi(X, \mathcal{F}) = \int_X \mathrm{Td}(\mathcal{T}_X)\mathrm{Ch}(\mathcal{F})$$

et $\mathrm{Td}(\mathcal{T}_X)\mathrm{Ch}(\mathcal{F}) \in \mathrm{Chow}(X) \otimes \mathbb{Z}[1/(2d)!]$. Or l'image de $\int_X : \mathrm{Chow}(X) \longrightarrow \mathbb{Z}$ est exactement $[X : K]\mathbb{Z}$, d'où la conclusion. □

Chapitre 6

Propriétés diophantiennes des corps

Ce chapitre est le cœur du mémoire. Il s'agit de définir des bonnes propriétés diophantiennes des corps toutes reliées à la question de l'existence de points rationnels sur une variété souvent définie par beaucoup de variables et avec un petit degré, et d'étudier comment se comportent ces propriétés lorsque l'on fait des opérations naturelles sur les corps : ajouter une indéterminée ou une indéterminée infinitésimale, passer aux vecteurs de Witt, prendre une extension algébrique...
Lang est le premier à définir de telles conditions avec la propriété C_i des corps. Cette condition est raffinée par Kato et Kuzumaki, qui définissent une propriété C_i^q qui fait intervenir les groupes de K-théorie de Milnor. Nous verrons aussi une condition C_1^q forte définie par Wittenberg qui porte non seulement sur les schémas projectifs, mais sur tous les schémas propres sur le corps de base.
La philosophie de la conjecture de Kato et Kuzumaki est alors de relier ces diverses propriétés à la dimension cohomologique de notre corps K. On veut par exemple que K soit C_i si et seulement s'il est de dimension cohomologique inférieure ou égale à i. Ce premier espoir est assez peu réaliste à cause des corps p-adiques, et la conjecture de Kato et Kuzumaki est plus précise.

Conjecture 6.0.0.1. *(Kato, Kuzumaki)*
Soit K un corps et i, q des entiers naturels. Les conditions suivantes sont équivalentes :

- *La dimension cohomologique de K est au plus $i+q$.*
- *Le corps K vérifie la condition C_i^q.*

Comme expliqué dans l'introduction, cette conjecture est toujours fausse avec des exemples très complexes, mais il est naturel de l'étudier pour les corps de la vraie vie.

Définition 6.0.0.2. *(Indice d'une variété)*
Dans tout ce chapitre, si X est une variété sur un corps K, on définit l'indice de X sur K, noté parfois $[X : K]$ comme le pgcd *des degrés des extensions de K où X possède un K-point. Si X est vide, cet indice vaut donc 0.*

6.1 Condition C_i de Lang

Définition 6.1.0.1. *(Lang) Soit $i \geq 0$ un entier. Un corps k est C_i si pour tous $n \geq 1$ et $d \geq 1$ vérifiant $d^i \leq n$, toute hypersurface de degré d dans $\mathbb{P}^n_k$ possède un k-point. De façon plus élémentaire, tout polynôme homogène de degré d à $n+1$ variables à un zéro non-trivial dans k.*

Un corps est C_0 si et seulement si il est algébriquement clos, et le théorème de *Chevalley-Warning* entraîne que les corps finis sont C_1.

Notons que $C_0 \implies C_1 \implies C_2 \implies \ldots$.
La proposition suivante est l'un des premiers liens observés entre les propriétés C_i et la dimension cohomologique des corps.

Proposition 6.1.0.2. *Soit k un corps C_1. Alors toute algèbre centrale simple sur k est déployée, autrement dit* $\mathrm{Br}(k) = 0$.

Démonstration. Il suffit de montrer que la seule algèbre à division centrale finie D sur k est k. Or on dispose de la norme réduite $N : D \longrightarrow k$ qui forme un polynôme homogène de degré d à d^2 variables si $[D : k] = d^2$. Comme k est C_1, cette norme s'annule en un $x \in D \setminus \{0\}$, contredisant $1 = N(xx^{-1}) = N(x)N(x^{-1})$. □

De cette observation, on obtient directement le théorème de Wedderburn.

Corollaire 6.1.0.3. *(Wedderburn) Tout anneau à division fini est commutatif.*

Un outil essentiel pour étudier la propriété C_i est la notion de *forme normique* définie dans [5], chapitre 3.

Définition 6.1.0.4. *Soit k un corps. Une forme normique est un polynôme homogène f de degré d à d variables qui ne s'annule qu'en* 0 *sur le corps k.*
Si ℓ/k est une extension finie de degré d, la norme de ℓ, $N_{\ell/k}$, est une forme normique.

Lemme 6.1.0.5. *Si k n'est pas algébriquement clos, il possède des formes normiques de degré arbitrairement grand.*

Démonstration. Il existe ℓ/k une extension finie non-triviale, qui donne lieu à une première forme normique φ de degré $d > 1$. On considère alors :

$$\psi = \varphi(\varphi \mid \cdots \mid \varphi)$$

ce qui signifie $\psi(X_{i,j}) = \varphi(\varphi(X_{11},\ldots,X_{d1}),\ldots,\varphi(X_{1d},\ldots,X_{dd}))$. Ainsi ψ est une forme normique de degré d^2 et on peut itérer cette construction. □

Ceci permet d'établir le théorème suivant qui permet d'établir l'existence de points rationnels sur des intersections d'hypersurfaces de même degré sur un corps C_i.

Théorème 6.1.0.6. *(Lang-Nagata) Soit k un corps C_i et $f_1,\ldots,f_r$ des polynômes homogènes de même degré $d \geq 1$ à n variables avec $rd^i < n$. Alors f possède un* 0 *non-trivial dans k.*

Démonstration. Si k est algébriquement clos, le résultat s'obtient par la théorie de la dimension. Sinon, il existe φ une forme normique de degré $e \geq r$, et on pose alors :

$$\varphi_1 = \varphi(f_1, f_2,\ldots,f_r \mid f_1,\ldots,f_r \mid \cdots \mid f_1,\ldots,f_r \mid 0,\ldots 0)$$

où l'on place strictement moins que r fois le 0 à la fin. Encore une fois, le symbole | signifie que l'on utilise de nouvelles variables. Ainsi φ_1 est un polyôme homogène à $\left\lfloor \frac{e}{r} \right\rfloor n$ variables et de degré ed. On itère la construction :

$$\varphi_{m+1} = \varphi_m(f_1, f_2,\ldots,f_r \mid f_1,\ldots,f_r \mid \cdots \mid f_1,\ldots,f_r \mid 0,\ldots 0)$$

de sorte que, si D_m est le degré de φ_m et N_m est le nombre de variables de φ_m, on ait :

$$D_m = ed^m$$

et

$$N_{m+1} = \left\lfloor \frac{N_m}{r} \right\rfloor n \geq \left(\frac{N_m}{r} - 1 \right) n$$

ce qui donne :

$$N_m \geq \left(\frac{n}{r} \right)^m C + A$$

avec $C > 0$ et $A \in \mathbb{R}$ (on peut commencer la récurrence à $m = 1$ pour avoir un premier terme strictement positif). Puisque $\frac{n}{r} \geq \frac{rd^{i+1}}{r} > d^i$, on a à partir d'un certain rang $N_m > D_m^i$ et puisque k est C_i on trouve un zéro non-trivial de $\varphi^{(m)}$ ce qui assure que les f_i ont un zéro commun non-trivial. □

Ce théorème permet notamment de démontrer le résultat suivant qui permet de relier les propriétés arithmétiques d'un corps k à celles de ses extensions de degré de transcendance fini.

Corollaire 6.1.0.7. *Soit ℓ/k une extension de corps de degré de transcendance fini r. Si k est un corps C_i, alors ℓ est un corps C_{i+r}.*

Démonstration. On se ramène aux deux résultats suivants : si k est C_i alors $k(T)$ est C_{i+1} et si ℓ/k est une extension algébrique alors ℓ est encore C_i.
Commençons par le premier : on se donne f un polynôme homogène à coefficients dans $k(T)$ à n variables et de degré d avec $d^{i+1} < n$. On peut supposer que f est à coefficients dans $k[T]$. On cherche à résoudre, pour $g_1, \ldots, g_n \in k[T]$:

$$f(g_1(T), \ldots, g_n(T)) = 0$$

avec $g_i = x_{i0}T^0 + \cdots + x_{is}T^s$ avec s à choisir ensuite. On obtient une équation en développant :

$$f_0(x_{ij}) + f_1(x_{ij})T + \cdots + f_{ds+r}(x_{ij})T^{ds+r}$$

avec r le maximum des degrés (en T) des coefficients du polynôme f. Les f_k sont des polynômes homogènes de degré d en $(s+1)n$ variables, donc si $(ds+r+1)d^i < (s+1)n$, comme k est C_i, on trouve une solution non-triviale à notre système par le théorème de Lang-Nagata 6.1.0.6. Or cette condition est facile à réaliser en choisissant s assez grand.
Ensuite, supposons ℓ/k algébrique. On se ramène facilement au cas où ℓ/k est finie car f vit dans un corps intermédiaire fini sur k. On se donne alors $(e_1, \ldots, e_m)$ une k-base de ℓ et, si f est homogène de degré d avec $d^i < n$, on doit résoudre $f(x_1, \ldots, x_n) = 0$, et on décompose alors chaque x_i dans la base $\underline{e}$, ce qui donne $x_i = \sum_j x_{ij} e_j$ et en décomposant l'équation dans la base, on obtient un système de m équations homogènes de degré d à mn variables, que l'on sait résoudre car k est C_i et par Lang-Nagata. □

En combinant ce théorème avec la proposition 6.1.0.2, on obtient un théorème de Tsen.

Corollaire 6.1.0.8. *(Tsen) Si k est algébriquement clos, alors* $\mathrm{Br}(k(T)) = 0$.

Avec les mêmes méthodes qu'avant et en utilisant le théorème d'approximation de Greenberg ci-dessous 6.1.0.9 on montre aussi que si un corps k est C_i, alors le corps $k((T))$ est C_{i+1}.

Théorème 6.1.0.9. *(Théorème d'approximation de Greenberg) Soit K un corps à valuation discrète d'anneau de valuation R d'idéal maximal* $\mathfrak{m}$*. On suppose K complet (ou plus généralement,* $\mathcal{O}_K$ *hensélien excellent). Soit* $\mathcal{X}$ *un R-schéma de type fini. Alors* $\mathcal{X}$ *possède un point sur R si et seulement si* $\mathcal{X}$ *possède un point dans* $R/\mathfrak{m}^k$ *pour tout* $k \geq 1$*.*

En réalité, le théorème de Greenberg dit mieux que ça et affirme qu'il suffit d'avoir des points dans les $R/\mathfrak{m}^k$ pour k assez grand, avec une borne précise. On renvoie à l'article de Greenberg [6] pour l'énoncé plus général et sa preuve.
Dans le cas où les caractéristiques sont différentes, mais seulement pour $i = 0$, on a aussi le résultat suivant de Lang. On renvoie au chapitre 6 du livre de Greenberg [5] pour les détails.

Théorème 6.1.0.10. *(Lang) Soit K un corps complet de valuation discrète de corps résiduel k algébriquement clos. Alors K est un corps* C^1*.*

Remarque 6.1.0.11. Comme beaucoup d'énoncés sur les corps complets, on peut supposer quelque chose de plus faible, à savoir que le lemme de Hensel soit valable dans K. On en déduit par exemple que l'extension maximale non-ramifiée de $\mathbb{Q}_p$ est un corps C^1.

6.2 Corps p-spéciaux

La notion de corps p-spécial sera utile dans la suite pour relier les conditions C_i et C_i^q.
On rappelle que si ℓ/k est une extension algébrique, on peut définir son degré de la façon suivante :

$$[\ell : k] = \mathrm{ppcm}_f [f : k]$$

où le ppcm porte sur toutes les extensions finies intermédiaires de k, et est un nombre surnaturel, c'est à dire un élément de $\prod_p (\mathbb{N} \cup \infty)$. Si ℓ/k est galoisienne, alors $[l : k]$ est exactement l'ordre du groupe profini $\mathrm{Gal}(\ell/k)$ (voir 1.2.1.4). Enfin, si $m/\ell/k$ est une tour d'extensions algébriques, on a :

$$[m : k] = [m : \ell][\ell : k]$$

et on renvoie à [15] pour une preuve de ce fait.

Définition 6.2.0.1. *Soit p un nombre premier. Un corps k est p-spécial si toute extension finie de k est de degré une puissance de p.*

Proposition 6.2.0.2. *Soit k un corps et p un nombre premier. Il existe une unique extension algébrique* $k(p)$ *de k à k-isomorphisme près qui soit un corps p-spécial et tel que toute extension intermédiaire* $k(p)/\ell/k$ *finie* (ℓ/k) *soit de degré premier à p.*
De plus, si $p = \mathrm{car}(k)$ *ou si k est parfait, alors* $k(p)$ *est une extension séparable de k associée à un pro-p-Sylow de* G_k*, et sinon,* $k(p)$ *est la clôture parfaite d'une telle extension.*

Démonstration. On fixe $k_s \subseteq \overline{k}$ des clôture séparable et algébrique de k respectivement. Par le lemme de Zorn, il existe $k(p)$ une extension algébrique de k maximale pour la propriété que $[k(p) : k]$ est premier à p. Montrons que $k(p)$ est un corps p-spécial. Soit $\ell/k(p)$ une extension finie. Si elle est séparable, on peut la supposer galoisienne de groupe G et on veut voir que G est un p-groupe. Or G vérifie la propriété suivante, par maximalité de $k(p)$: tout sous-groupe strict de G est d'indice divisible par p. Ainsi, un p-Sylow de G est égal à G, sinon son indice serait divisible par p et ce ne serait pas un p-Sylow. Donc G est un p-groupe.

Si $\ell/k(p)$ n'est pas séparable, on peut considérer ℓ' la clôture séparable de $k(p)$ dans ℓ. Par ce qui précède, $[\ell' : k(p)]$ est une puissance de p et il faut voir que $[\ell : \ell']$ en est aussi une. Si $p = \mathrm{car}(k)$, c'est clair. Sinon, on a $\ell = \ell'$ car le corps $k(p)$ est alors parfait : en effet, si $q = \mathrm{car}(k) > 0$, et si $x^{1/q} \notin k(p)$ pour un $x \in k(p)$, on trouve une extension de $k(p)$ de degré q en adjoignant $x^{1/q}$, ce qui contredit la maximalité de $k(p)$. Ceci démontre l'existence d'une telle extension.
Voyons l'unicité à présent. Si k est parfait ou de caractéristique p, alors un tel corps $k(p)$ est une extension séparable de k et donc correspond nécessairement à un pro-p-Sylow de G_k, et deux pro-p-Sylow sont conjugués. Si k est de caractéristique $q \neq p$ positive, alors $k(p)$ est nécessairement la clôture parfaite du corps correspondant à un pro-p-Sylow de G_k, donc deux tels corps sont isomorphes. □

Remarque 6.2.0.3. Soit ℓ/k une extension algébrique. En adaptant la preuve précédente, on peut montrer que $k(p)$ se plonge dans $\ell(p)$ au dessus de k.

6.3 Condition C_i^q

On commence par introduire des notations qui nous seront très utiles dans la suite.

Définition 6.3.0.1. *Soient $q \geq 0$ un entier et k un corps.*
Si Z est un k-schéma de type fini, on définit le q-ème groupe de normes de Z, $N_q(Z/k) \subseteq K_q(k)$ le sous-groupe de $K_q(k)$ engendré par les images des morphismes $N_{\ell/k} : K_q(\ell) \longrightarrow K_q(k)$ pour toutes les extensions finies ℓ telles que $Z(\ell) \neq \emptyset$. Si f est un polynôme homogène définissant une hypersurface projective X, on pose aussi $N_q(f/k) = N_q(X/k)$.
Soit maintenant p un nombre premier fixé, $n \geq 0$ un entier et $\alpha \in K_n(k)/pK_n(k)$. On définit de façon analogue le q-ème groupe de normes de α, $N_q(\alpha/k) \subseteq K_q(k)$ engendré par les images des morphismes $N_{\ell/k} : K_q(\ell)/p \longrightarrow K_q(k)/p$ pour toutes les extensions ℓ telles que $\alpha_{|\ell} = 0 \in K_n(\ell)/pK_n(\ell)$. On définit aussi le q-ème noyau de α, noté $\mathrm{Ker}_q(\alpha)$ comme l'ensemble des $\beta \in K_q(k)$ qui vérifient :

$$\{\alpha, \beta\} = 0 \ [p].$$

Il est clair qu'on a alors $\alpha \in \mathrm{Ker}_n(\beta) \iff \beta \in \mathrm{Ker}_q(\alpha)$.

Proposition 6.3.0.2. *Pour tout $\alpha \in K_n(k)/pK_n(k)$, on a :*

$$N_q(\alpha/k) \subseteq \mathrm{Ker}_q(\alpha).$$

Démonstration. Soit ℓ/k une extension finie dans laquelle $\alpha_{|\ell} = 0 \ [p]$ et soit $x = N_{\ell/k}(y) \in K_q(k)$ une norme non-nulle pour cette extension. On a alors :

$$\{x, \alpha\} = N_{\ell/k}\left\{y, \alpha_{|\ell}\right\} = 0 \ [p]$$

□

Définition 6.3.0.3. *Soient $q \geq 0$ et $i \geq 0$. On dit qu'un corps k est C_i^q si pour toute extension finie ℓ/k et tout f homogène de degré d à coefficients dans ℓ avec $n > d^i$ variables, on a :*

$$N_q(f/\ell) = K_q(f/\ell).$$

Parfois, nous aurons besoin de la propriété $C_i^q(d)$, celle où l'on allège la condition C_i^q en ne supposant que la condition pour des hypersurfaces de degré d. On définit la condition $C_i(d)$ de façon similaire.
Notons que si $i' \geq i$ et $q' \geq q$, alors $C_i^q \implies C_{i'}^{q'}$ grâce à la formule de projection, et remarquons que la définition est construite de telle sorte qu'elle soit stable par passage à une extension finie.
Commençons par comprendre les cas limites $i = 0$ ou $q = 0$.

Remarque 6.3.0.4. (Le cas limite $q = 0$)
La condition C_i^0 équivaut à ce que, pour toute extension finie ℓ/k et toute hypersurface Z de $\mathbb{P}_\ell^n$ de degré d avec $d^i \leq n$, Z possède un 0-cycle de degré 1 : c'est à dire une somme formelle de points fermés de Z dont le degré vale 1. Par Bézout, cela revient encore à dire que les degrés des extensions résiduelles de Z sont premiers entre eux dans leur ensemble.
En particulier, le théorème de Springer 4.5.0.5 entraîne que :

$$C_i^0(2) \iff C_i(2).$$

Remarque 6.3.0.5. La condition C_i^q est censée être stable par passage à une extension algébrique, mais je n'ai pas trouvé de bonne explication dans la littérature. En effet, supposons que k est un corps C_i^q et que ℓ/k est une extension algébrique. Puisqu'une extension finie de ℓ est encore une extension algébrique de k, il suffit de montrer la condition diophantienne directement pour ℓ. Soit donc X une hypersurface de $\mathbb{P}_\ell^n$ définie par un polynôme homogène f de degré d avec $d^i \leq n$. Il s'agit de voir que :

$$N_q(X/\ell) = K_q(\ell).$$

Il existe une extension finie m/k contenue dans ℓ telle que f soit à coefficients dans m, et comme k est C_i^q, on a :

$$N_q(f/m) = K_q(m).$$

Soit alors $\alpha \in K_q(\ell)$. Quitte à agrandir m, on peut supposer que α provient de $K_q(m)$. On trouve alors des extensions finies m_i/m où f s'annule et des $\alpha_i \in K_q(m_i)$ tels que :

$$\prod_i N_{m_i/m}(\alpha_i) = \alpha \in K_q(m).$$

Il s'agit alors de définir la K-théorie de la ℓ-algèbre finie $\ell \otimes_m m_i$ et d'étendre les morphismes normes à ce cas là en vérifiant qu'ils vérifient toujours les mêmes propriétés, afin d'avoir :

$$N_{m_i/m}(\alpha_i)_{|\ell} = N_{m_i \otimes_m \ell/\ell}(\alpha_i) \in K_q(\ell)$$

ce qui fonctionnerait au moins dans le cas où m_i/m est séparable.

Proposition 6.3.0.6. *Le corps k est C_0^q si et seulement si pour toute tour d'extensions finies $m/\ell/k$, le morphisme :*

$$N_{m/\ell} : K_q(m) \longrightarrow K_q(\ell)$$

est surjectif.
Si k est un corps p-spécial comme défini en 6.2.0.1, alors la condition C_i^0 équivaut à la condition C_i. Plus généralement, un corps k est C_i^0 si et seulement si pour tout nombre premier p, le corps $k(p)$ défini en 6.2.0.2 est un corps C_i.

Démonstration. En effet, si k est C_0^q, on veut voir que $K_q(m) \longrightarrow K_q(\ell)$ est surjectif et par fonctorialité on se ramène au cas où $m = \ell[x]$, avec P le polynôme minimal de x sur ℓ, et il suffit alors de considérer l'hypersurface Z projectivisée de l'hypersurface affine $P(x) = 0$ dans $\mathbb{P}^1$. La réciproque est claire.
Ensuite, il est clair qu'un corps C_i est C_i^0 puisque la condition C_i^0 demande l'existence de 0-cycles de degré 1, ce qui est moins fort que l'existence de points rationnels.
Si pour un certain nombre premier p, k est p-spécial, alors en retour on a l'implication $C_i^0 \implies C_i$ car le seul moyen d'avoir un 0-cycle de degré 1 dans ce cas est d'avoir un point rationnel car si des

puissances de p sont premières entre elles, alors l'une d'elles vaut 1.
Ainsi, si k est C_i^0 alors les corps $k(p)$ sont C_i^0 car cette propriété est stable par extension algébrique, et donc par l'observation précédente $k(p)$ est C_i. Réciproquement, si tous ces corps sont C_i, et si ℓ/k est une extension finie et Z une hypersurface de $\mathbb{P}_\ell^n$ de degré d avec $d^i \leq n$, alors pour tout premier p on peut supposer $k(p) \subseteq \ell(p)$ d'après la remarque 6.2.0.3 de sorte que $\ell(p)$ est une extension algébrique de $k(p)$, donc $\ell(p)$ est un corps C_i et donc Z possède un point dont le degré sur ℓ est premier à p. Ceci étant vrai pour tout p, les degrés résiduels de Z sur ℓ sont donc premiers entre eux. □

La conjecture de Bloch-Kato ou théorème de Voevodsky 4.7.0.2 permet de démontrer le lien suivant entre dimension cohomologique et propriété C_0^q.

Théorème 6.3.0.7. *Soit k un corps de caractéristique nulle et $q \geq 0$ un entier. Les propositions suivantes sont équivalentes :*

— *Le corps k est C_0^q.*

— *Le corps k est de dimension cohomologique au plus q.*

Plus généralement, si p est un nombre premier différent de la caractéristique de k, on a toujours $C_0^q \implies \mathrm{cd}_p(k) \leq q$.

Démonstration. Supposons que k est C_0^q et soit p un nombre premier différent de la caractéristique de k. Comme la condition C_0^q est stable par passage à une extension algébrique, on peut supposer que G_k est un pro-p-Sylow. Dans ce cas, il suffit de montrer que :

$$H^{q+1}(G_k, \mu_p^{q+1}) = 0$$

d'après 2.5.0.4. Or par Bloch-Kato 4.7.0.2 :

$$H^{q+1}(G_k, \mu_p^{q+1}) \cong K_{q+1}(k)/pK_{q+1}(k).$$

Soit donc $\{a_1, \ldots, a_{q+1}\} \in K_{q+1}(k)$ et montrons que cet élément est divisible par p. Pour cela on considère $\ell = k(a_{q+1}^{1/p})$ qui est une extension finie de k et comme k est C_0^q, il existe $u \in K_q(\ell)$ vérifiant :

$$\left\{a_1, \ldots, a_q\right\} = N_{\ell/k}(u)$$

de sorte que $\left\{a_1, \ldots, a_{q+1}\right\} = pN_{\ell/k}\left\{u, a_{q+1}^{1/p}\right\}$ comme souhaité.
Ensuite, supposons k de caractéristique nulle et $\mathrm{cd}(k) \leq q$ et montrons que k est C_0^q. Il suffit de montrer que pour toute extension finie ℓ/k, la norme sur les groupes K_q est surjective car la deuxième proposition est stable par passage aux extensions algébriques (séparables).
Notons d le degré de l'extension ℓ/k. Puisque $dK_q(k) \subseteq N(K_q(\ell))$, il suffit de montrer que :

$$K_q(\ell)/d \longrightarrow K_q(k)/d$$

est surjective. Or, par Bloch-Kato, cela revient à la surjectivité du morphisme correspondant :

$$H^q(\ell, \mu_d^{\otimes q}) \longrightarrow H^q(k, \mu_d^{\otimes q})$$

dont on se convainc facilement qu'il s'agit du morphisme de restriction en cohomologie. Puisque G_ℓ est d'indice fini dans G_k, on a une suite exacte de la forme :

$$0 \longrightarrow I \longrightarrow \mathrm{Coind}_{G_\ell}^{G_k} \mu_d^{\otimes q} \longrightarrow \mu_d^{\otimes q} \longrightarrow 0$$

avec I de torsion, qui donne bien la surjectivité voulue en appliquant le lemme de Shapiro et le fait que $H^{q+1}(G_k, I) = 0$. □

Remarque 6.3.0.8. Le théorème précédent reste valable en caractéristique positive, en utilisant la bonne définition de dimension cohomologique en la caractéristique. On renvoie à [14] pour ce cas là.

On peut montrer certains liens entre les propriétés C_i et C_i^q.

Proposition 6.3.0.9. *Soit p un nombre premier, k un corps de caractéristique différente de p qui contient les racines p-èmes de l'unité et A une algèbre centrale simple finie sur k dont la classe dans le groupe de Brauer est annulée par p. On note $N_r : A \longrightarrow k$ la norme réduite de A et on a alors :*

$$N_1(\alpha_A/k) = N_r(A^\times)$$

avec $\alpha_A \in K_2(k)/pK_2(k)$ l'élément qui correspond à $[A] \in H_2(k, \mu_p)$ par l'isomorphisme de Bloch-Kato 4.7.0.2.

Démonstration. Par Bloch-Kato, A est déployée sur une extension finie ℓ/k si et seulement si $(\alpha_A)_\ell = 0\ [p]$. Il s'agit donc de montrer l'égalité suivante :

$$N_r(A^\times) = \langle N_{\ell/k}(\ell^\times) \mid [A_{|\ell}] = 0 \rangle.$$

Notons que si $A = M_n(D)$ avec D une algèbre à division centrale, la norme réduite de A se factorise par celle de D avec le déterminant $M_n(D) \longrightarrow D$ qui est surjectif, de sorte qu'on peut supposer que $A = D$ est une algèbre à division centrale finie sur k. Ainsi, si $x \in D^\times$, il existe un corps ℓ contenant $k(x)$ qui est maximal dans D et donc D se déploye dans ℓ, et on a bien :

$$N_r(x) = N_{\ell/k}(x).$$

Ensuite, si ℓ/k déploye D, il existe $B = M_m(D)$ une algèbre centrale simple sur k dans laquelle ℓ se plonge et est strictement maximal (i.e. $[B : k] = [\ell : k]^2$) de sorte que :

$$N_r(D^\times) = N_r(B^\times) \supseteq N_{\ell/k}(\ell^\times).$$

□

Théorème 6.3.0.10. *Soit k un corps et p un nombre premier différent de la caractéristique de k. Si k est C_i, alors il est aussi C_i^0, et on a de plus les implications suivantes :*

$$C_1 \implies \mathrm{cd}_p(k) \leq 1$$

et

$$C_2 \implies \mathrm{cd}_p(k) \leq 2$$

et ainsi, si k est de caractéristique nulle, $C_1 \implies C_0^1$ et $C_2 \implies C_0^2$. Encore une fois, il existe une généralisation à la caractéristique positive.

Démonstration. On a déjà vu que $C_i \implies C_i^0$. Dans les deux cas à traiter, on peut remplacer k par k_s^H avec H un pro-p-Sylow de G_k d'après 2.5.0.4, et ainsi on a $\mu_p \subseteq k$ et il suffit de considérer la cohomologie de μ_p.
Dans le premier cas, si k est C_1, alors on veut voir que :

$$H^2(k, \mu_p) = 0.$$

Or la proposition 6.1.0.2 assure que $\mathrm{Br}(k) = 0$ et permet de conclure.
Supposons maintenant que k est C_2. On commence par observer que si D est une algèbre à division

centrale finie sur k de dimension d^2, la norme réduite $N_r : D \longrightarrow k$ est un polynôme homogène à d^2 variables et de degré d, de sorte que pour tout $\lambda \in k^\times$, l'équation homogène $N_r(X_{i,j}) = \lambda T^d$ à d^2+1 variables possède une solution non-triviale, et comme D est une algèbre à division, une telle solution vérifie $T \neq 0$. On en déduit que N_r est surjective. Ensuite, si A est une algèbre centrale simple finie sur k, on a $A \cong M_n(D)$ avec D une algèbre à division centrale et la norme réduite de A se factorise en $M_n(D) \xrightarrow{\det} D \xrightarrow{N_r} k$, donc encore une fois $N_r : A \longrightarrow k$ est surjective.
On fixe un isomorphisme de G_k-modules entre μ_p et $\mathbb{Z}/p\mathbb{Z}$ puisque $\mu_p \subseteq k$. Ainsi, si $a,b,c \in k^\times/(k^\times)^p$, on sait que $a \in N_r(A)$ avec A l'algèbre centrale simple correspondant à $b \cup c \in H^2(k,\mu_p)$, or on a montré que $N_r(A) = N_1(\{b,c\}/k) \subseteq \mathrm{Ker}(\{b,c\}/k)$ de sorte que $\{a,b,c\} = 0$, et par Bloch-Kato 4.7.0.2, ceci démontre que $H^3(k,\mu_p) = 0$.

□

6.4 Formes de Pfister et dimension cohomologique en $p = 2$

Soit k un corps de caractéristique différente de 2. On définit la condition $C_i^q(\mathrm{Pf})$ suivante : k est $C_i^q(\mathrm{Pf})$ si pour toute extension finie ℓ/k, pour tout $n > i$ et pour toute forme de Pfister φ à 2^n variables sur ℓ, on a $K_q(\ell) = N_q(\varphi/\ell)$. C'est simplement la condition C_i^q où n'autorise seulement les hypersurfaces définies par des formes de Pfister. Le but de cette partie est de démontrer la proposition suivante, due à Kato et Kuzumaki dans l'article [14].

Proposition 6.4.0.1. *Soit k un corps de caractéristique différente de 2. Pour tout $j \geq 0$, les conditions $C_i^q(\mathrm{Pf})$ avec $i+q=j$ sont deux à deux équivalentes, et sont aussi équivalentes à :*

$$\mathrm{cd}_2(k) \leq j.$$

Pour cela, on va se baser sur l'isomorphisme de Milnor 4.6.0.2 qui permet de relier les éléments de K-théorie de Milnor et les formes de Pfister. On utilise les notations de la partie sur les formes de Pfister. Soit $\varphi = \langle\langle a_1,\dots,a_n\rangle\rangle \in I^n$ une forme de Pfister et $\alpha = \{a_1,\dots,a_n\} \in K_n(k)/2$ le symbole correspondant. Un résultat non-trivial de Lam et Elman (voir [24], théorème 3.2) affirme que deux formes de Pfister φ et φ' sont égales modulo I^{n+1} si et seulement si elles sont isométriques. En particulier, $\{a_1,\dots,a_n\} = 0$ [2] si et seulement si $\langle\langle a_1,\dots,a_n\rangle\rangle$ est isotrope sur k et ainsi $\varphi_{|\ell} = 0$ si et seulement si $\alpha_{|\ell} = 0$ pour ℓ/k une extension finie. On en déduit la proposition suivante.

Proposition 6.4.0.2. *Soit k un corps de caractéristique différente de 2 et $a_1,\dots,a_n \in k^\times/(k^\times)^2$. On a alors pour tout $q \geq 0$:*

$$N_q(\langle\langle a_1,\dots,a_n\rangle\rangle/k) = N_q(\{a_1,\dots,a_n\}/k) \subseteq K_q(k)/2$$

où la norme est prise pour le nombre premier 2.

On montre même mieux : les symboles purs du q-noyau proviennent du groupe des q-normes (voir 6.3.0.1) pour un symbole de Milnor pur modulo 2.

Proposition 6.4.0.3. *Soit k un corps de caractéristique différente de 2 et $a_1,\dots,a_n \in k^\times/(k^\times)^2$. On a alors pour tout $q \geq 0$:*

$$\mathrm{Ker}_q(\{a_1,\dots,a_n\})_{\mathrm{pur}} \subseteq N_q(\{a_1,\dots,a_n\}) \subseteq K_q(k)/2$$

où l'indice pur signifie qu'on ne prend que les symboles purs (qui a priori ne forment pas un sous-groupe).

Pour cela, on commence par énoncer un lemme classique sur les valeurs prises par une forme quadratique.

Lemme 6.4.0.4. *Soit φ une forme quadratique sur k qui représente 1. On rappelle que $D(\varphi)$ désigne l'ensemble des valeurs non-nulles prises par φ. On a alors l'inclusion suivante :*

$$D(\varphi) \subseteq N_1(\varphi/k).$$

Démonstration. On peut clairement supposer φ anisotrope. Soit $a \in D(\varphi)$. On peut rendre φ isotrope dans une extension quadratique (si $\varphi = \langle a_1, \dots, a_n \rangle$, elle devient isotrope dans $k(\sqrt{-a_1/a_2})$ par exemple) et donc si a est un carré l'énoncé est évident. On suppose à présent que a n'est pas un carré, et on choisit $v \neq 0$ un vecteur tel que $\varphi(v) = a$, et $w \neq 0$ tel que $\varphi(w) = 1$. Comme a n'est pas un carré, la famille (v, w) est libre. Puisque φ est anisotrope, on obtient :

$$\varphi = \langle 1, a \rangle \oplus \psi.$$

On peut donc supposer $\varphi = \langle 1, a \rangle$. On considère alors l'extension $\ell = k(\sqrt{-a})$ dans laquelle φ devient anisotrope (et donc $-a$ n'est pas un carré dans k) car :

$$\sqrt{-a}^2 + a = 0$$

et on a :

$$N_{\ell/k}(\sqrt{-a}) = a$$

comme voulu. □

Ce lemme s'applique en particulier aux formes de Pfister car elles représentent toutes 1.
On démontre à présent la proposition 6.4.0.3.

Démonstration. Soient $a_1, \dots, a_n \in k^\times$. On montre d'abord que si $\{a_1, \dots, a_i\} \in N_i(\{a_{i+1}, \dots, a_n\}/k)$, alors $\{a_1, \dots, a_{i+1}\} \in N_{i+1}(\{a_{i+2}, \dots, a_n\}/k)$ pour $0 \leq i \leq n-2$.
Notons $\varphi = \langle\langle a_{i+1}, \dots, a_n \rangle\rangle$ et $\psi = \langle\langle a_{i+2}, \dots, a_n \rangle\rangle$ de sorte que :

$$\varphi = \psi \oplus \langle -a_{i+1} \rangle \psi.$$

On écrit $\{a_1, \dots, a_i\} = \sum_j N_{\ell_j/k}(u_j)$ avec φ isotrope sur chaque ℓ_j. Comme φ est isotrope sur ℓ_j, et que $D(\psi \otimes \ell_j)$ est un groupe - puisque ψ est une forme de Pfister - on obtient :

$$a_{i+1} \in D(\psi \otimes \ell_j) \subseteq N_1(\psi/\ell_j)$$

par le lemme 6.4.0.4. Ainsi $\{a_1, \dots, a_{i+1}\}$ est dans le groupe :

$$\sum_j \left\{ N_{\ell_j/k}(K_i(\ell_j)), N_1(\psi/\ell_j) \right\}$$

et la formule de projection permet de s'assurer que ce groupe est contenu dans $N_{i+1}(\psi/k)$ comme souhaité : en effet, il s'agit de voir que si $m/\ell/k$ est une tour d'extension, si $u \in K_*(\ell)$ et $v \in K_*(m)$ tel que $N_{m/\ell}(v) = (a_{i+1})_\ell$, alors :

$$N_{m/k}(u_m v) = N_{\ell/k}(N_{m/\ell}(u_m v)) = N_{\ell/k}(u N_{m/\ell}(v)) = N_{\ell/k}(u(a_{i+1})_\ell) = N_{\ell/k}(u) a_{i+1}.$$

Ensuite, il est clair que :

$$N_0(\{a_1, \dots, a_n\}) = \mathrm{Ker}_0(\{a_1, \dots, a_n\}).$$

Ceci permet de conclure : si $\left\{a_1, \dots, a_q\right\} \in \mathrm{Ker}_q(\left\{a_{q+1}, \dots, a_n\right\})$, alors $\{a_1, \dots, a_n\} = 0$ et donc $1 \in N_0(\{a_1, \dots, a_n\})$ puis $a_1 \in N_1(\{a_2, \dots, a_n\})$ et ainsi de suite. □

La proposition 6.4.0.1 découle directement de la proposition 6.4.0.3.

Démonstration. D'abord, remarquons que $\mathrm{cd}_2(k) \leq j \implies C_0^j(\mathrm{Pf})$ puisque pour tout $\{a_1,\dots,a_j\} \in K_j(k)/2$ et pour toute forme de Pfister $\langle\langle a_{j+1},\dots,a_{j+n}\rangle\rangle$ à 2^n variables avec $n \geq 1$, on a par Bloch-Kato $K_{j+n}(k)/2 \cong H_{j+n}(k,\mu_2) = 0$ et donc $\{a_1,\dots,a_n\} = 0$ et on utilise 6.4.0.3 pour conclure. Les deux conditions étant stables par passage à une extension finie, on n'a pas besoin de le remontrer pour ℓ/k une extension finie.
Ensuite, si $C_i^q(\mathrm{Pf})$ est vérifié par k avec $i+q=j$, c'est aussi vérifié par toute extension algébrique de k et ainsi on peut supposer que k est 2-spécial (voir 6.2.0.1) pour montrer que $\mathrm{cd}_2(k) \leq j$. Il suffit alors, comme d'habitude, de montrer que $H^{j+1}(k,\mu_2) = 0$, autrement dit, par Bloch-Kato 4.7.0.2, que $\{a_1,\dots,a_{j+1}\} = 0$ [2] pour tous $a_i \in k^\times$. Or, k étant $C_i^q(\mathrm{Pf})$, on a $\{a_1,\dots,a_q\} \in N_q(\langle\langle a_{q+1},\dots,a_{j+1}\rangle\rangle/k) \subseteq \mathrm{Ker}_q(\{a_{q+1},\dots,a_{j+1}\})$, d'où la conclusion. □

Il est naturel de se demander comment généraliser $C_1 \implies C_0^1$ et $C_2 \implies C_0^2$. La remarque suivante explique une tentative naturelle mais insuffisante qui utilise des produits tensoriels de polynômes.

Remarque 6.4.0.5. Supposons que k contienne les racines p-ème de l'unité et soit de caractéristique différente de p. Dans les preuves du théorème 6.3.0.10 et de la proposition 6.4.0.1, l'ingrédient principal est la construction, pour chaque symbole pur $\alpha = \{a_1,\dots,a_q\} \in K_q(k)$ avec $q \geq 0$ et p un nombre premier différent de la caractéristique de k, d'un polynôme homogène f à coefficients dans k de degré p et à p^q variables tel que f s'annule sur ℓ une extension finie de k si et seulement si $\alpha_{|\ell} = 0$ dans $K_q(\ell)/p$. Disons d'un tel polynôme, s'il existe, que c'est un polynôme de déploiement du symbole α.

Le succès des preuves précédentes vient du fait qu'on sait construire un tel polynôme de déploiement quand $q=1$ (il s'agit de la norme de la k-algèbre étale $k[T]/(T^p-a_1)$) et quand $q=2$ (prendre la norme réduite de l'algèbre cyclique $a_1 \cup a_2$ associée au symbole $\alpha = \{a_1,a_2\}$), ainsi que quand $p=2$ grâce aux formes de Pfister : on prend alors pour forme de déploiement associée à $\{a_1,\dots,a_q\}$ la forme de Pfister $\langle\langle a_1,\dots,a_q\rangle\rangle$.
On peut naturellement se demander si la construction des formes de déploiement fonctionne plus généralement. Une idée intuitive, au moins en caractéristique strictement plus grande que p, est la suivante : si $\alpha = \{a_1,\dots,a_q\}$, on considère f_i le polynôme de déploiement de $\{a_i\}$ modulo p, c'est à dire la norme de $k[T]/(T^p-a_i)$, puis on considère le produit tensoriel $f_1 \otimes \cdots \otimes f_q$ de ces polynômes, qui est défini de la façon suivante :

Soient V et W deux k-espaces vectoriels de dimension finie. Si la caractéristique de k est strictement plus grande que p, on peut identifier l'espace $\mathrm{Sym}^p(V^*)$ des polynômes homogènes de degré p sur V à celui des p-formes symétriques $(\mathrm{Sym}^p V)^*$, et on a alors un produit tensoriel canonique $(\mathrm{Sym}^p V)^* \otimes (\mathrm{Sym}^p W)^* \longrightarrow (\mathrm{Sym}^p(V\otimes W))^*$ qui à $f\otimes g$ associe la forme p-symétrique qui envoie $(v_1\otimes w_1,\dots,v_p\otimes w_p)$ sur $f(v_1,\dots,v_p)g(w_1,\dots,w_p)$. Ce produit tensoriel induit, via l'identification faite précedemment, un produit tensoriel au niveau des polynômes homogènes de degré p. Quand $p=2$, on retrouve le produit tensoriel des formes quadratiques.

Cependant, pour $p \neq 2$, la définition n'est pas satisfaisante : on s'attendrait à ce que, si $a,b \in k^\times$, et si f_a et f_b sont les normes des algèbres étales $k[T]/(T^p-a)$ et $k[T]/(T^p-b)$, alors le polynôme $f_a \otimes f_b$ soit la norme réduite h de l'algèbre cyclique $a\cup b$, mais ce n'est pas tout à fait le cas après vérification

numérique pour $p = 3$. Il semblerait toutefois, que si $k = \mathbb{Q}(\mu_p)$, on ait $f_a \otimes f_b = \mathrm{Tr}_{k/\mathbb{Q}}(h)$.
En général, il n'est pas clair qu'un tel polynôme de déploiement existe, et il faut en général construire des *variétés* de déploiement (voir [12]).

Chapitre 7

Transition des propriétés diophantiennes du corps résiduel au corps des fractions d'un anneau de valuation discrète

Soit K un corps muni d'une valuation discrète v, que l'on va supposer ici *complet* et de corps résiduel k *parfait* pour faciliter des réductions techniques (voir [14] pour le cas général où K est seulement supposé d'anneau d'entiers hensélien excellent).
On s'intéresse ici aux liens entre les propriétés C_i^q sur K et sur k. Rappelons que dans le cas équicaractéristique, c'est à dire lorsque $K = k((T))$ on a le résultat suivant : si k est C_i, alors K est C_{i+1}. Ceci suggère qu'en général on ait : si k est C_i^q, alors K est C_i^{q+1} et C_{i+1}^q.
On va voir quelques résultats positifs dans ce sens d'abord dans l'article de Kato et Kuzumaki [14] et puis dans l'article de Wittenberg pour une condition C_i^q un peu différente, dite forte.
Commençons par rappeler que l'on a une suite exacte, pour tout $q \geq 1$:

$$0 \longrightarrow U_q(K) \longrightarrow K_q(K) \xrightarrow{\partial} K_{q-1}(k) \longrightarrow 0$$

avec les notations de 4. Cette suite exacte induit, pour X un K-schéma de type fini, une suite exacte :

$$0 \longrightarrow \frac{U_q(K)}{U_q(K) \cap N_q(X/K)} \longrightarrow \frac{K_q(K)}{N_q(X/K)} \longrightarrow \frac{K_{q-1}(k)}{\partial N_q(X/K)} \longrightarrow 0$$

qui sera souvent utile pour démontrer des propriétés de transition entre k et K.

7.1 Propriétés de transition pour la propriété C_i^q

On aura besoin du lemme suivant qui provient de [14]. On dira parfois qu'un polynôme homogène *s'annule* sur un corps s'il a un zéro non-trivial défini sur ce corps.

Lemme 7.1.0.1. *Supposons k infini (et parfait) et soit f un polynôme homogène de degré $d \geq 1$ à coefficients dans $\mathcal{O}_K$ et à $n \geq 1$ variables. On suppose que $\overline{f}$ ne s'annule pas dans le corps k et on se donne ℓ/k une extension finie où il s'annule. Alors il existe L/K une extension finie telle que ℓ se plonge dans le corps résiduel $\kappa(L)$ de L au dessus de k, f s'annule sur L et :*

$$\frac{[L:K]}{[\ell:k]} < d.$$

Démonstration. Comme k est supposé parfait, on peut écrire $\ell = k[\alpha]$ et il existe alors $g_1, \dots, g_n \in \mathcal{O}_K[T]$ de degrés $d_i < [\ell : k]$ tels que :

$$f(g_1(\alpha), \dots, g_n(\alpha)) = 0$$

dans ℓ. On pose alors $\varphi(T) = f(g_1(T), \dots, g_n(T))$ et on note que $\overline{\varphi} \neq 0$ car k est infini et $\overline{f}$ ne s'annule pas sur k. Puisque $\overline{\varphi}(\alpha) = 0$, il existe un facteur $\psi \mid \varphi$ dans $\mathcal{O}_K[T]$ dont l'image dans $k[T]$ est irréductible tel que $\overline{\psi}(\alpha) = 0$ et on peut alors considérer le corps $L = K[T]/(\psi)$ dont le corps résiduel $\kappa(L)$ contient bien un conjugué de α sur k. Par construction, f s'annule sur L puisque $\varphi(T)$ est nulle dans L. Enfin, on a bien :

$$[L : K] = \deg(\psi) \leq \deg(\varphi) < d[\ell : k].$$

□

Notons que dans ce lemme, on a $[\ell : k] \mid [\kappa(L) : k] \mid [L : K]$ donc $\frac{[L:K]}{[\ell:k]}$ est en fait un entier.
On peut à présent démontrer le théorème suivant.

Théorème 7.1.0.2. *Soit K un corps à valuation discrète v, complet, de corps résiduel k parfait et soit p un nombre premier. Alors k est un corps $C_i^0(p)$ si et seulement si K est un corps $C_{i+1}^0(p)$.*

Démonstration. On commence par traiter le cas où le corps résiduel k est infini. On s'y ramènera ensuite.
Supposons que k est $C_i^0(p)$ et donnons-nous L/K une extension finie. Il s'agit de montrer que si f à coefficients dans L est de degré p à n variables avec $p^{i+1} < n$, alors l'hypersurface associée Z a un 0-cycle de degré 1. Puisque $\kappa(L)$, le corps résiduel de L, est une extension finie de k, il est aussi $C_i^0(p)$ et donc on peut oublier ce corps L et supposer $L = K$. Ainsi dans la suite f est à coefficients dans K.
D'après le lemme suivant 7.1.0.3, il suffit de montrer que l'hypersurface X définie par f possède un 0-cycle de degré premier à p. On suppose le contraire et on définit une valuation sur K^n de la façon suivante :

$$v_f(x) = \frac{1}{p} v(f(x))$$

avec v la valuation du corps K. Vérifions que ça définit bien une valuation de K-espace vectoriel. On a clairement $v_f(\lambda x) = v(\lambda) + v_f(x)$ et $v_f(x) = \infty \iff x = 0$ car 0 est le seul point d'annulation de f par hypothèse. Il reste à vérifier l'inégalité ultramétrique :

$$v_f(x + y) \geq \min(v_f(x), v_f(y)).$$

On peut supposer que (x, y) est libre et que $v_f(x) \leq v_f(y)$. Considérons $g(T) = f(Tx + y)$ qui est irréductible de degré p sur K par l'hypothèse faite sur f. Si α est une racine de g et $L = K(\alpha)$, alors $g(T) = N_{L/K}(T - \alpha) f(x)$ car $f(x)$ est le coefficient dominant de g. Ainsi :

$$f(x + y) = f(x) N_{L/K}(1 - \alpha)$$

et puisque $N_{L/K}(-\alpha) = \frac{f(y)}{f(x)} \in \mathcal{O}_K$, on a $\alpha \in \mathcal{O}_L$ et donc $f(x) \mid f(x + y)$, d'où $v_f(x + y) \geq v_f(x)$.
De là, on peut considérer les boules fermées $V^{(m)} = f^{-1}(\mathfrak{m}_K^m)$ pour $m \geq 0$ et comme les normes sont équivalentes en dimension finie sur un corps *complet*, $V^{(m)}$ est un $\mathcal{O}_K$-module libre de rang fini n qui engendre K-linéairement K^n, autrement dit c'est un $\mathcal{O}_K$-réseau de K^n. Notons que pour tout m, le quotient $W_m = V^{(m)}/V^{(m+1)}$ est un k-espace vectoriel de dimension finie, et que, si π est une uniformisante de K, le polynôme $\pi^{-m} f$ induit une fonction polynomiale homogène de degré p, f_m :

$W_m \longrightarrow k$. Plus précisément, si $e_1, \dots, e_r \in V^{(m)}$ induisent une k-base de W_m, alors f_m correspond à la réduction dans $k[T_1, \dots, T_r]$ du polynôme $F_m = \pi^{-m} f(T_1 e_1 + \cdots + T_r e_r)$ qui est bien à coefficients entiers car il est à valeurs entières sur les entiers et le corps résiduel k est *infini*.
Par construction, f_m ne s'annule qu'en 0 sur W_m. Par le lemme 7.1.0.1 appliqué à F_m, on obtient que f_m ne s'annule sur aucune extension ℓ/k de degré premier à p : en effet, si f_m s'annule sur une telle extension L/K, le lemme assure que F_m s'annule sur une extension L/K avec :

$$\mathbb{Z} \ni \frac{[L:K]}{[\ell:k]} < p.$$

Mais par hypothèse sur f, on a $p \mid [L:K]$ et $p \nmid [\ell:k]$ donc p divise ce quotient, et c'est absurde.
On en déduit que f_m n'a pas de zéro-cycle de degré 1 et comme k est un corps $C_i^0(p)$, on a :

$$\dim W_m \leq p^i$$

pour tout $m \geq 0$. Or, comme $V^{(0)}$ est un $\mathcal{O}_K$-réseau de K^n :

$$p^{i+1} < n = \dim_k(V^{(0)}/\mathfrak{m}_K V^{(0)}) = \dim_k(V^{(0)}/V^{(p)}) = \sum_{j=0}^{p-1} \dim_k W^{(j)} \leq p^{i+1}$$

ce qui est absurde.
Réciproquement, supposons que K est un corps $C_{i+1}^0(p)$. Encore une fois, par compatibilité aux extensions algébriques et parce que toute extension finie de k se relève en une extension finie (non-ramifiée par exemple) de K, on se ramène à montrer que si g est un polynôme homogène à $n > p^i$ variables à coefficients dans k de degré p, alors l'hypersurface définie par g possède un 0-cycle de degré 1.
On choisit G un relevé de g homogène de degré p à coefficients dans $\mathcal{O}_K$ et on considère :

$$f = \sum_{j=0}^{p-1} \pi^j G(X_{j,1}, \dots, X_{j,n})$$

qui est homogène de degré p à np variables. Puisque K est $C_{i+1}^0(p)$, f a un zéro-cycle de degré 1 sur K donc s'annule sur une extension L/K de degré premier à p. On en déduit facilement (en prenant une solution primitive dans $\mathcal{O}_L$) que g s'annule sur l'extension résiduelle et que X a un zéro-cycle de degré 1 encore avec le lemme 7.1.0.3.
Il reste enfin à expliquer comment on se ramène au cas où le corps résiduel k est infini. Rappelons que l'hypothèse $C_i^0(p)$ est équivalente, par 6.3.0.6, à la condition $C_i^0(p)$ pour certaines extensions qui sont des corps infinis, ce qui permet la réduction voulue. Plus précisément, si q est un nombre premier, il correspond à l'extension séparable $k(q)$ de k (voir 6.2.0.2) une extension non-ramifiée $K(q)$ de K de corps résiduel $k(q)$ dont toute extension finie intermédiaire est de degré premier à q, et on peut montrer avec la même preuve que 6.3.0.6 que si tous ces $K(q)$ vérifient $C_{i+1}^0(p)$, alors K aussi. □

On a utilisé le lemme suivant.

Lemme 7.1.0.3. *Soit k un corps infini et X une hypersurface de $\mathbb{P}^n$ de degré $d \geq 1$. Alors X possède un 0-cycle de degré d.*

Démonstration. L'hypersurface X est le lieu d'annulation d'un polynôme homogène f de degré d. On commence par montrer qu'il existe un changement de variable linéaire qui permet d'écrire $f = X_1^d + g$ avec $u \neq 0$ et g qui ne fait apparaître que des termes de degré au plus $d-1$ en X_1. Pour cela, il suffit de montrer que si le nombre minimal de variables d'un monôme apparaissant dans f est $\ell \geq 2$, alors il existe un changement de variables qui donne un nombre minimal de variables d'un monôme apparaissant dans f d'au plus $\ell - 1$. Dans ce qui suit, on peut supposer que f possède un monôme de la forme $X_1^{\beta_1} \dots X_\ell^{\beta_\ell}$ avec chaque $\beta_i \geq 1$. Écrivons :

$$f = \sum_{|\alpha|=d} a_\alpha \underline{X}^\alpha$$

la somme portant sur les multi-indices de degré d. On effectue le changement de variable suivant :

$$X_1 = Y_1 + \lambda Y_2$$

et $X_i = Y_i$ pour $i \geq 2$, avec $\lambda \in k$ un paramètre. On a donc :

$$\begin{aligned} f &= \sum_{|\alpha|=d} \sum_{j=0}^{\alpha_1} \binom{\alpha_1}{j} a_\alpha \lambda^{\alpha_1 - j} Y_1^j Y_2^{\alpha_1 - j + \alpha_2} Y_3^{\alpha_3} \dots Y_n^{\alpha_n} \\ &= \left(\sum_\gamma \lambda^{\gamma_1} \right) Y_2^{\beta_1 + \beta_2} Y_3^{\beta_3} \dots Y_\ell^{\beta_\ell} + \dots \end{aligned}$$

où les … ne font pas apparaître ce premier monôme et la somme porte sur les multi-indices γ de degré d tels que $\gamma_i = \beta_i$ pour $i \geq 3$ et $\gamma_1 + \gamma_2 = \beta_1 + \beta_2$. Comme k est infini, il existe λ tel que $\sum_\gamma \lambda^{\gamma_1} \neq 0$ car c'est un polynôme non-nul en λ.
On peut donc supposer $f = X_1^d + g$ comme décrit plus haut, et ainsi en choisissant des valeurs quelconques $x_2, \dots, x_n$ pour $X_2, \dots, X_n$ dans k, on factorise $f(T, x_2, \dots, x_n) = f_1(T) \dots f_r(T)$ en produit d'irréductibles dans $k[T]$ et on en déduit en prenant des racines des f_i dans des extensions de k de degrés $d_i = \deg(f_i)$ que X possède un 0-cycle de degré $\sum d_i = d$. □

On a traité le cas limite $q = 0$, et on s'occupe à présent du cas limite $i = 0$. Encore une fois, l'hypothèse de caractéristique nulle du corps résiduel peut être supprimée et on peut supposer $\mathcal{O}_K$ hensélien excellent plutôt que complet (voir [14] pour l'énoncé complet).

Théorème 7.1.0.4. *Soit K un corps à valuation discrète complet de corps résiduel k de caractéristique nulle, autrement dit K est le corps des séries de Laurent sur k. Alors le corps k est C_0^q si et seulement si K est C_0^{q+1}.*

Démonstration. On reprend les notations de la partie 4 sur la K-théorie de Milnor.
Supposons que K est un corps C_0^{q+1}. Puisque cette condition est stable par passage aux extensions finies et que toute extension finie de k se relève en une extension (non-ramifiée) de K, il suffit de montrer que pour toute extension finie ℓ/k, le morphisme :

$$N_{\ell/k} : K_q(\ell) \longrightarrow K_q(k)$$

est surjectif. On considère L/K l'extension non-ramifiée associée à ℓ/k et on a un diagramme commutatif dont les colonnes sont données par les morphismes surjectifs de résidu (voir 4.3.0.2) :

$$\begin{array}{ccc} K_{q+1}(L) & \xrightarrow{N_{L/K}} & K_{q+1}(K) \\ \partial\downarrow & & \downarrow\partial \\ K_q(\ell) & \xrightarrow[N_{\ell/k}]{} & K_q(k) \end{array}$$

et ce diagramme prouve cette première implication.
Supposons à présent que k est un corps C_0^q et donnons-nous L/K une extension finie de degré d. On note ℓ le corps résiduel de L. Il suffit de montrer que $N_{L/K} : K_{q+1}(L)/dK_{q+1}(L) \longrightarrow K_{q+1}(K)/dK_{q+1}(K)$ est surjectif, puisque l'image du morphisme norme contient toujours $dK_{q+1}(K)$. Comme d est inversible dans k, on a un diagramme commutatif (voir 4.2.0.4) :

$$\begin{array}{ccc} K_{q+1}(L)/dK_{q+1}(L) & \xrightarrow{N_{L/K}} & K_{q+1}(K)/dK_{q+1}(K) \\ {\scriptstyle (s_{\pi_L},\partial)}\downarrow & & \downarrow{\scriptstyle (s_{\pi_K},\partial)} \\ K_{q+1}(\ell)/dK_{q+1}(\ell)\oplus K_q(\ell)/dK_q(\ell) & \xrightarrow[\varphi]{} & K_{q+1}(k)/dK_{q+1}(k)\oplus K_q(k)/dK_q(k) \end{array}$$

avec des uniformisantes π_K et π_L de K et L et e l'indice d'inertie de L/K. Les colonnes sont des isomorphismes, et puisque k est C_0^q et de caractéristique nulle, sa dimension cohomologique est au plus q d'après 6.3.0.7, et donc par Bloch-Kato $K_{q+1}(k)/dK_{q+1}(k) = 0$ (ou plus simplement en reprenant la preuve de 6.3.0.7). Ainsi, au regard de la proposition 4.3.0.2, le morphisme horizontal du bas devient simplement $N_{\ell/k}$, qui est surjectif car k est C_0^q. Le morphisme du dessus est donc aussi surjectif.

□

Corollaire 7.1.0.5. *Avec les mêmes notations que dans le théorème précédent et grâce à 6.3.0.7, on en déduit que :*

$$\mathrm{cd}(K) = \mathrm{cd}(k) + 1.$$

Enfin, voyons ce qu'il est possible de dire dans un cas où $i \neq 0$ et $q \neq 0$.

Théorème 7.1.0.6. *Soit K un corps parfait à valuation discrète v, complet, de corps résiduel k parfait et soit p un nombre premier. On suppose que k est un corps $C_i^{q-1}(p)$ et $C_{i-1}^q(p)$ pour $i, q \geq 1$. Alors le corps K est $C_i^q(p)$.*

Démonstration. Comme dans la preuve de 7.1.0.2, on se ramène facilement au cas où le corps résiduel k est *infini*. Soit f un polynôme homogène de degré p à $n > p^i$ variables sur K (on se ramène à ce cas par les arguments habituels de passage à une extension finie). On veut voir :

$$N_q(f/K) = K_q(K).$$

Si f a un zéro dans une extension L/K de degré premier à p, il n'y a rien à faire car $pK_q(K)$ est contenu dans $N_q(f/k)$ puisque, par le lemme 7.1.0.3, f possède un 0-cycle de degré p, et donc il existe des corps d'annulation de f, L_i/K de degrés d_i et une relation de Bézout $\sum_i u_i d_i = p$ qui donne pour tout symbole $px \in pK_q(K)$:

$$px = \sum_i u_i d_i x \in \sum_i N_q(L_i/K) \subseteq N_q(f/k).$$

On suppose à présent que f ne s'annule dans aucune extension de degré premier à p, et ainsi on peut introduire les $V^{(m)}$ comme dans la preuve de 7.1.0.2. De l'égalité :

$$n = \sum_{m=0}^{p-1} \dim_k W^{(m)}$$

on déduit qu'il existe $0 \leq m < p$ avec $\dim_k W^{(m)} > p^{i-1}$. Puisque k est $C_{i-1}^q(p)$, le polynôme f_m défini comme dans 7.1.0.2 vérifie :

$$N_q(f_m/k) = K_q(k).$$

On rappelle alors que le morphisme de spécialisation induit un isomorphisme :

$$U_q(K)/U_q^1(K) \cong K_q(k).$$

L'extension maximale non-ramifiée K^{nr} de K est un corps C^1 par le théorème de Lang 6.1.0.10 et la remarque 6.1.0.11 en utilisant le fait que k est parfait, en particulier f possède un 0 non-trivial dans une extension finie non-ramifiée L de K, puisque $p < n$. La norme induite sur les unités $\mathcal{O}_L^\times \longrightarrow \mathcal{O}_K^\times$ est surjective car l'extension est non-ramifiée, et donc tout élément de $U_q^1(K)$ se relève par la norme (en effet $U_q^1(K)$ est engendré par les $\{x_1, \ldots, x_n\}$ avec $x_1 \in U^1(K)$ et il suffit de relever x_1). On a ainsi :

$$U_q^1(K) \subseteq N_q(f/K).$$

En utilisant le lemme 7.1.0.1, on a alors :

$$U_q(K) \subseteq N_q(f/K)U_q^1(K) = N_q(f/K) \quad (*).$$

À présent, deux cas sont possibles :

— S'il existe $0 \leq u < v < p$ avec $W^{(u)} \neq 0$ et $W^{(v)} \neq 0$, alors on prend $x \in V^{(u)} \setminus V^{(u+1)}$ et $y \in V^{(v)} \setminus V^{(v+1)}$. Le polynôme $h(T) = \pi^{-u} f(Tx + y)$ envoie $\mathcal{O}_K$ dans $\mathcal{O}_K$ donc, comme k est infini, est à coefficients dans $\mathcal{O}_K$. De plus, par construction, le polynôme réduit $\overline{h} \in k[T]$ ne s'annule qu'en 0 dans $\overline{k}$, et donc h est multiple d'un polynôme d'Eisenstein et s'annule sur une extension L/K totalement ramifiée. Ainsi f s'annule dans L et comme l'extension est totalement ramifiée, la norme sur les extensions résiduelles est un isomorphisme et donc par le diagramme commutatif 4.3.0.2, on obtient :

$$K_q(K) = N_{L/K}(K_q(L)) + \operatorname{Ker} \partial = N_{L/K}(K_q(L)) + U_q(K)$$

et on conclut avec $(*)$.

— Il existe un seul $0 \leq u < p$ avec $W^{(u)} \neq 0$. Dans ce cas, on a :

$$\dim W^{(u)} = n > p^i$$

donc en définissant $f^{(u)}$ comme au dessus et en utilisant que k est un corps $C_i^{q-1}(p)$, on a :

$$K_{q-1}(k) = N_{q-1}(f^{(u)}/k).$$

On conclut alors comme avant grâce à 7.1.0.1.

□

7.2 Propriétés de transition pour la propriété C_1^q forte de Wittenberg en dehors de la caractéristique résiduelle

On introduit, selon Wittenberg, la propriété C_1^q forte ainsi que les propriétés C_1^q fortes en un nombre premier p et en dehors de p, qui sont plus souples que la propriété C_1^q. On verra que les corps p-adiques vérifient la condition C_1^1 forte en dehors de p et la condition C_1^1.

Définition 7.2.0.1. *(Propriété C_1^q forte de Wittenberg)*
Soit K un corps. On dit que K vérifie la propriété C_1^q forte si pour toute extension finie L/K et tout L-schéma propre X, on a :

$$[X:K]_\chi \cdot \Big(K_q(L)/N_q(X/L)\Big) = 0$$

autrement dit l'exposant du groupe de torsion $K_q(L)/N_q(X/L)$ divise l'indice cohomologique $[X:K]_\chi$ (voir 5.2.0.1) (on rappelle que ce groupe est annulé par l'indice $[X:L]$ par l'argument usuel de restriction-corestriction).
Si p est un nombre premier, on raffine cela en deux notions différentes :
On dit que K vérifie la propriété C_1^q forte en p (respectivement en dehors de p) si, avec les mêmes quantifications qu'au dessus, la divisibilité de l'exposant de $\Big(K_q(L)/N_q(X/L)\Big)$ par $[X:K]_\chi$ a lieu dans $\mathbb{Z}_p$ (resp. dans $\mathbb{Z}[1/p]$).

Puisque les hypersurfaces intervenant dans la définition de la propriété C_1^q de Kato et Kuzumaki ont une caractéristique d'Euler égale à 1, la condition C_1^q forte entraîne la condition C_1^q.
Wittenberg démontre alors dans son article [30] un résultat analogue à 7.1.0.6, résultat qui nous permettra notamment d'affirmer que les corps p-adiques sont C_1^1 en dehors de p, ce qui servira ensuite à montrer que les corps de nombres totalement imaginaires sont C_1^1. Encore une fois, on choisit de se restreindre au cas de corps complets pour plus de simplicité.

Théorème 7.2.0.2. *(Wittenberg)*
Soit R un anneau de valuation discrète complet de corps des fractions K et de corps résiduel k, et soit ℓ non-nul dans k. Soit $q \geq 1$ un entier. Si k vérifie la condition C_1^{q-1} forte en ℓ et C_0^q en ℓ (i.e. $\mathrm{cd}_\ell(k) \leq q$), alors K vérifie la propriété C_1^q forte en ℓ.
En particulier, tout corps p-adique vérifie la propriété C_1^1 forte en $\ell \neq p$.

Pour comprendre la preuve de ce théorème, on a besoin d'un peu plus d'outils sur la géométrie sur un anneau de valuation discrète.

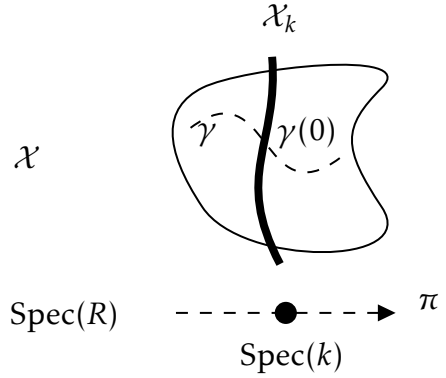
7.2.1 Arithmétique des schémas sur un anneau de valuation discrète

Soit R un anneau de valuation discrète de corps des fractions K et de corps résiduel k et soit π une uniformisante de R. Le schéma $\mathrm{Spec}(R)$ est alors, du point de vue topologique, la réunion disjointe du fermé $\mathrm{Spec}(k)$ et de l'ouvert $\mathrm{Spec}(K) = D(\pi)$.
Géométriquement, on peut le voir comme un *trait infinitésimal* avec un point au milieu. Ainsi, si $\mathcal{X}$ est un schéma sur $\mathrm{Spec}(R)$, on a aussi une décomposition de $\mathcal{X}$ en la fibre spéciale $\mathcal{X}_k$, fermée, et la fibre générale $\mathcal{X}_K$, ouverte.
La fibre spéciale est une hypersurface définie par l'équation $p^*\pi = 0$ avec $p : \mathcal{X} \longrightarrow \mathrm{Spec}(R)$ le morphisme structural, et la fibre générale est l'ouvert $p^*\pi \neq 0$.

Si $\mathcal{X}$ est propre sur Spec(R), le critère valuatif de propreté assure d'ailleurs que l'application canonique :

$$\mathcal{X}(R) \longrightarrow \mathcal{X}(K)$$

est une bijection. Il est ainsi possible de réduire les points de $\mathcal{X}(K)$ dans $\mathcal{X}(k)$.
On peut donner une interprétation géométrique pour clarifier tout ceci : $\mathcal{X}$ est une famille de schémas qui varient au dessus du trait infinitésimal Spec(R), paramétrés par la coordonnée π. En $\pi = 0$, on retrouve la fibre spéciale et en $\pi \neq 0$, on a la fibre générique. Un k-point de $\mathcal{X}$ est un point de la fibre spécial défini sur k, un R-point de $\mathcal{X}$ est une courbe infinitésimale γ qui traverse $\mathcal{X}$ dans la direction donnée par Spec(R), et l'application : $\mathcal{X}(R) \longrightarrow \mathcal{X}(k)$ est l'évaluation du chemin γ en la coordonnée $\pi = 0$.



D'autre part, un K-point de $\mathcal{X}$ est la donnée d'une courbe infinitésimale qui parcourt $\mathcal{X}$ dans la direction donnée par π mais avec un éventuel pôle en $\pi = 0$. Si $\mathcal{X}$ est propre, un tel pôle ne peut pas exister à cause du critère valuatif, d'où le fait que $\mathcal{X}(R) = \mathcal{X}(K)$.
Si R est complet, alors pour toute extension finie séparable L/K on peut former S la clôture intégrale de R dans L, qui est encore un anneau de valuation discrète complet avec une valuation qui étend celle de R définie de façon unique. Dans ce cas, si $\mathcal{X}$ est propre sur R, $\mathcal{X}_S$ est propre sur S et donc on a aussi une bijection :

$$\mathcal{X}(S) \cong \mathcal{X}(L).$$

On en déduit le lemme suivant, qui assure que l'on peut toujours réduire un point fermé de $\mathcal{X}_K$ en un point fermé de $\mathcal{X}_k$ bien défini, si $\mathcal{X}$ est propre sur R.

Lemme 7.2.1.1. *(Réduction des points fermés)*
Soit R un anneau de valuation discrète complet et $\mathcal{X}$ un schéma propre sur R. Pour tout point fermé x de $\mathcal{X}_K$, il existe un unique point fermé $[x]$ de $\mathcal{X}_k$ dans Z, l'adhérence de x dans $\mathcal{X}$.

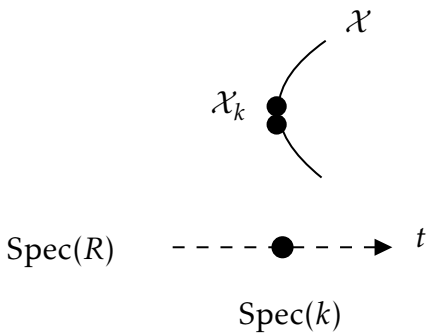
La fibre spéciale $\mathcal{X}_k$ n'a pas de raison d'être régulière ou même réduite, ce qui amène à la définition suivante.

Définition 7.2.1.2. *(Multiplicité de la fibre spéciale) Soit R un anneau de valuation discrète de corps résiduel k et corps des fractions K et soit $\mathcal{X}$ un R-schéma de type fini. On définit la multiplicité de la fibre spéciale comme le plus grand entier $m \geq 1$ tel que le diviseur de $p^*\pi$ soit divisible par m dans le groupe des diviseurs de $\mathcal{X}$. Si $\mathcal{X}_k$ est irréductible, c'est la longueur de l'anneau artinien $\mathcal{O}_{\mathcal{X}_k,\eta}$ avec η le point générique de $\mathcal{X}_k^{\text{red}}$.*

Exemple 7.2.1.3. Prenons k un corps quelconque de caractéristique différente de 2 et $R = k[[t]]$. Considérons alors le R-schéma de type fini suivant :

$$\mathcal{X} = \operatorname{Spec} R[x]/(x^2 - t).$$

Ce schéma peut se représenter comme le voisinage infinitésimal de la parabole $x^2 - t$ près de $t = 0$:



La fibre spéciale est ici un point double, c'est le diviseur de x^2, donc 2 fois le diviseur premier x, d'où une multiplicité de 2.

Du point de vue de la géométrie arithmétique et des propriétés diophantiennes des corps $\mathbb{Q}_p$, la question qui nous intéresse est alors la suivante :
Si $\mathcal{X}$ est un schéma propre sur R un anneau de valuation discrète complet, quel est le lien entre les points rationnels de $\mathcal{X}_K$ et les points rationnels de $\mathcal{X}_k$?
Dans cette question, le mot point rationnel est à comprendre en un sens vague : on s'intéresse aux points définis sur des extensions pas trop grandes. Une question plus précise consiste à chercher un lien entre l'indice $[\mathcal{X}_k : k]$ et l'indice $[\mathcal{X} : K]$, ou plutôt l'indice *résiduel* de $\mathcal{X}$ sur K, noté $[\mathcal{X} : K]_{\text{res}}$ défini comme le pgcd des degrés d'inertie des extensions finies de K où $\mathcal{X}$ possède un point.
On rappelle que le degré d'inertie d'une extension L/K est le degré de l'extension résiduelle ℓ/k associée.
Le lemme 7.2.1.1 assure alors une première relation de divisibilité :

$$[\mathcal{X}_k : k] \mid [\mathcal{X} : K]_{\text{res}}$$

pour $\mathcal{X}$ un R-schéma propre. L'autre relation n'est pas valable en général, mais Wittenberg démontre tout de même qu'elle l'est pour certains schémas : d'une part les schémas réguliers et plats de type fini sur R (quand k est infini) et d'autre part les quotients par un groupe fini de schémas réguliers projectifs et plats sur R (quand k est fini). Ces deux cas seront utiles respectivement pour obtenir la propriété C_1^1 des corps p-adiques en dehors de p et en p.

Proposition 7.2.1.4. *Soit R un anneau de valuation discrète complet de corps des fractions K et de corps résiduel k et $\mathcal{X}$ un schéma sur* Spec(R) *qui vérifie l'une des deux conditions suivantes.*

- *$\mathcal{X}$ est plat, régulier, de type fini sur R, et le corps résiduel k est infini.*
- *$\mathcal{X}$ est le quotient par un groupe fini d'un schéma projectif, régulier et plat sur R, et le corps résiduel k est fini.*

Alors on a :

$$[\mathcal{X} : K]_{\text{res}} \mid [\mathcal{X}_k : k].$$

On ne vas ici présenter qu'une esquisse de preuve du résultat de Wittenberg, en mettant en avant l'aspect géométrique, car les détails algébriques sont plutôt techniques.

Démonstration. Commençons par le premier point. On montre un peu mieux : si x est un point fermé de la fibre spéciale $\mathcal{X}_k$, alors $\mathcal{X}_K$ possède un point fermé $\widehat{x}$ telle que le corps résiduel du corps à valuation discrète $K(\widehat{x})$ soit le corps $k(x)$.
Pour cela, on commence par se ramener au cas où la fibre spéciale réduite $\mathcal{X}_k^{\mathrm{red}}$ est régulière en x de la façon suivante : on considère $\mathcal{Y} \xrightarrow{p} \mathcal{X}$ l'éclatement de $\mathcal{X}$ en le point fermé x dont le diviseur exceptionnel est un espace projectif sur R. On cherche alors un point fermé y de $\mathcal{Y}_k \subseteq \mathcal{Y}$ dont le corps résiduel soit le corps $k(x)$ et qui se trouve sur une seule composante irréductible de $\mathcal{Y}_k$. Un tel point existe car k est infini (les fermés $Z \cap W$ avec Z et W composantes irréductibles distinctes de $\mathcal{Y}_k$ ne recouvrent pas l'espace projectif au niveau des $k(x)$-points).
Comme l'éclatement ne change pas $\mathcal{X}_K$ (il est réalisé en un point de la fibre spéciale qui est disjointe de la fibre générique), on peut supposer, quitte à remplacer $\mathcal{X}$ par $\mathcal{Y}$, que $\mathcal{X}_k^{\mathrm{red}}$ est régulier en x.
Expliquons géométriquement ce que l'on souhaite faire à présent : on a un point fermé régulier x de la fibre spéciale, et on souhaite tracer une courbe infinitésimale passant par x dont le corps résiduel du corps des fonctions soit $k(x)$. L'idée est que $\mathcal{X}_k$ est une hypersurface définie par $\pi = 0$, avec π une uniformisante de R, et donc $\mathcal{X}_k^{\mathrm{red}}$ est définie, au voisinage de x, par une équation $t = 0$ avec $t \in \sqrt{\pi \mathcal{O}_{\mathcal{X},x}}$. La régularité de $\mathcal{O}_{\mathcal{X}_k^{\mathrm{red}},x} = \mathcal{O}_{\mathcal{X},x}/(t)$ va permettre de construire une courbe transversale à $\mathcal{X}_k^{\mathrm{red}}$: on peut compléter t en un système régulier de paramètres $(t, f_1, \ldots, f_n)$ de l'anneau local $\mathcal{O}_{\mathcal{X},x}$, et considérer la courbe donnée au voisinage de x par les équations $f_i = 0$. Concrètement, il s'agit de considérer l'anneau de valuation discrète $S = \mathcal{O}_{\mathcal{X},x}/(f_1, \ldots, f_n)$ et de voir qu'il est fini sur R, de sorte que le morphisme canonique $\mathrm{Spec}(S) \longrightarrow \mathcal{X}$ est une immersion fermée car il provient du morphisme surjectif $\mathcal{O}_{\mathcal{X},x} \longrightarrow S$ qui s'étend localement autour de x de façon surjective par finitude de S.
Le point générique de $\mathrm{Spec}(S)$ est alors envoyé dans la fibre générique de $\mathcal{X}$ sur un point fermé de $\mathcal{X}_K$, qui a comme corps résiduel celui de S, c'est à dire $k(x)$.

On explique maintenant le second point : $\mathcal{X}$ est le quotient d'un schéma projectif, régulier et plat $\mathcal{Y}$ par l'action d'un groupe fini G. On note $q : \mathcal{Y} \longrightarrow \mathcal{X}$ la projection. Soit alors x un point fermé de $\mathcal{X}_k$, et $O = q^{-1}(x)^{\mathrm{red}}$ l'orbite réduite associée, qui est un fermé réduit de $\mathcal{Y}_k$. On fait éclater O, ce qui donne un schéma $\widehat{\mathcal{Y}}$ et un morphisme d'éclatement $\widehat{\mathcal{Y}} \xrightarrow{p} \mathcal{Y}$. Le groupe G agit encore sur $\mathcal{Z}$ par l'action tangente sur le diviseur exceptionnel, et on pose $\widehat{\mathcal{X}} = \widehat{\mathcal{Y}}/G$, de sorte qu'on a un diagramme commutatif de schémas sur R :

$$\begin{array}{ccc} \widehat{\mathcal{Y}} & \xrightarrow{p} & \mathcal{Y} \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q} \\ \widehat{\mathcal{X}} & \xrightarrow[p]{} & \mathcal{X} \end{array}$$

car p est G-équivariant. Puisque $\mathcal{Y}$ est régulier, le diviseur exceptionnel $E = p^{-1}(O)$ est un espace projectif $\mathbb{P}^n_O$ au dessus du schéma O, et G agit toujours sur E par l'action tangente. Notons que E est un $k(x)$-schéma. On montre à présent que E/G est géométriquement irréductible : si $\overline{k}$ est une clôture algébrique de k, on a :

$$E \otimes_{k(x)} \overline{k} = \mathbb{P}^n_{O \otimes_{k(x)} \overline{k}}$$

de sorte que les composantes irréductibles de $E \otimes_{k(x)} \overline{k}$ sont en bijection avec les composantes irréductibles du $\overline{k}$-schéma réduit $O \otimes_{k(x)} \overline{k}$ qui est fini sur $\overline{k}$, donc de dimension 0, et ainsi ces composantes

irréductibles correspondent aux $\overline{k}$-points de O. On montre alors que G agit transitivement sur les $\overline{k}$-points de O, ce qui n'est pas surprenant car O est une orbite du point de vue topologique.
Ainsi, lorsqu'on forme le quotient $E/G = q(E) \subseteq \widehat{\mathcal{X}}$, on obtient un schéma géométriquement irréductible de codimension 1 dans $\widehat{\mathcal{X}}$ car q est un morphisme fini et E est de codimension 1.
Comme $\widehat{\mathcal{X}}$ est un quotient d'un schéma normal par un groupe fini, il est encore normal (cela se vérifie au niveau des anneaux de fonctions en prenant les points fixes par l'action de G et en vérifiant que l'anneau obtenu reste intégralement clos). Ainsi, $\widehat{\mathcal{X}}$ est régulier en dehors d'un fermé de codimension au moins 2 et donc $\widehat{\mathcal{X}}$ est régulier en tout point d'un ouvert dense U de E/G.
On applique alors les bornes de Lang-Weil-Nisnevič (théorème 8.1.0.1), la finitude de k, et le fait que U est géométriquement intègre pour en déduire que U possède un point fermé y tel que $[k(y) : k]$ soit premier à $[\mathcal{X} : K]_{\text{res}}$.
En rétrécissant encore l'ouvert U, on peut faire en sorte que $\widehat{\mathcal{X}}$ et $\widehat{\mathcal{X}}_k^{\text{red}}$ soient réguliers en y, et on peut alors raisonner comme au dessus pour trouver un point fermé z de $\widehat{\mathcal{X}}_K$ tel que l'extension résiduelle de $K(z)/K$ soit $k(y)/k$. On a donc :

$$[\mathcal{X} : K]_{\text{res}} \mid [k(y) : k] = [k(y) : k(x)][k(x) : k]$$

et par lemme de Gauss, $[\mathcal{X} : K]_{\text{res}} \mid [k(x) : k]$. Ceci permet de conclure.

□

Voyons tout de suite un corollaire intéressant sur les morphismes résiduel en K-théorie de Milnor dû à Wittenberg.

Corollaire 7.2.1.5. *Soit R un anneau de valuation discrète complet de corps des fractions K et de corps résiduel k et $\mathcal{X}$ un schéma sur* Spec(R) *qui soit plat, régulier, et propre. Alors on a l'égalité suivante pour tout $q \geq 1$:*

$$\partial N_q(\mathcal{X}_K/K) = N_{q-1}(\mathcal{X}_k/k)$$

à l'intérieur du groupe $K_{q-1}(k)$.

Démonstration. L'inclusion de gauche à droite est élémentaire : si x est un L-point de $\mathcal{X}$ avec L/K une extension finie de corps résiduel ℓ/k, alors pour tout symbole $\alpha \in K_q(L)$, on a :

$$\partial N_{L/K}(\alpha) = N_{\ell/k}(\partial\alpha) \in N_{q-1}(\mathcal{X}_k/k)$$

car $\mathcal{X}_k$ possède un ℓ-point par propreté de $\mathcal{X}$, en réduisant le point x.
Montrons alors l'inclusion inverse. Soit donc $\beta = N_{\ell/k}(\gamma) \in N_{q-1}(\mathcal{X}_k/k)$ avec $\gamma \in K_{q-1}(\ell)$ et avec ℓ/k une extension finie où $\mathcal{X}$ possède un point. Si k est infini, la preuve de la proposition suivante 7.2.1.4 assure qu'il existe une extension finie L/K où $\mathcal{X}$ possède un point et dont le corps résiduel est ℓ. Il suffit alors d'observer le diagramme commutatif suivant 4.3.0.2 pour conclure :

$$\begin{array}{ccc} K_q(L) & \xrightarrow{\partial} & K_{q-1}(\ell) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{\ell/k}} \\ K_q(K) & \xrightarrow[\partial]{} & K_{q-1}(k) \end{array}$$

Il reste à traiter le cas où le corps résiduel k est fini en se ramenant au cas infini de la façon suivante. À cause de la suite exacte 7, le groupe $K_{q-1}(k)/\partial N_q(\mathcal{X}_K/K)$ est d'exposant fini donc il existe $n \geq 1$ tel que $n\beta \in \partial N_q(\mathcal{X}_K/K)$. On construit alors une tour infinie d'extensions $k = k_0 \subseteq k_1 \subseteq \ldots$ avec

k_{i+1}/k_i finie de degré premier à n. Il leur correspond des extensions non-ramifiées $K = K_0 \subseteq K_1 \subseteq \ldots$ d'anneaux d'entiers $R = R_0 \subseteq R_1 \subseteq \ldots$. On forme alors $K_\infty = \bigcup_i K_i$, $R_\infty = \bigcup_i R_i$ et $k_\infty = \bigcup_i k_i$. Puisque le corps k_∞ est infini, le cas précédent (qui est en fait encore valable pour un anneau de valuation discrète hensélien excellent, et R_∞ est excellent 7.2.1.6) appliqué à l'image β_∞ de β dans le groupe $N_{q-1}(\mathcal{X}_{k_\infty}/k_\infty)$ montre qu'il existe $\alpha_\infty \in N_q(\mathcal{X}_{K_\infty}/K_\infty)$ tel que $\partial\alpha_\infty = \beta_\infty$. Finalement, on trouve $\alpha_i \in N_q(\mathcal{X}_{K_i}/K_i)$ dont le bord est l'image β_i de β dans le groupe $K_{q-1}(\mathcal{X}_{k_i}/k_i)$. Ainsi, en prenant la norme, on a :

$$[k_i : k]\beta \in \partial(N_q(X/K))$$

et on conclut parce que $[k_i : k]$ est premier à n. □

Remarque 7.2.1.6. La raison pour laquelle l'anneau R_∞ dans la preuve ci-dessus est encore excellent est assez technique, mais dans la suite le cas qui nous intéresse est celui des corps p-adiques, et la question ne se pose alors même pas puisque ce sont des corps de caractéristique nulle. Une explication possible, due à mon encadrant D. Izquierdo, repose sur une caractérisation des anneaux henséliens excellents par la notion de F-finitude (voir [23], proposition 2.6.1).

Avec les mêmes notations qu'avant, on définit aussi l'indice de ramification de $\mathcal{X}$ comme le pgcd des degrés de ramification des extensions finies de K où $\mathcal{X}$ possède un point, et on le note $[\mathcal{X} : K]_{\text{ram}}$. Il est alors possible de démontrer que cet indice divise la multiplicité de la fibre spéciale hors de la caractéristique de k sous de bonnes hypothèses.

Proposition 7.2.1.7. *Soit R un anneau de valuation discrète complet de corps des fractions K et de corps résiduel k et $\mathcal{X}$ un schéma sur* Spec(R) *de type fini, régulier, irréductible, propre et plat. On a alors la divisibilité suivante dans l'anneau $\mathbb{Z}$ si k est de caractéristique nulle et dans l'anneau $\mathbb{Z}[1/p]$ si $p > 0$ est la caractéristique de k :*

$$[\mathcal{X} : K]_{\text{ram}} \mid \mu$$

avec μ la multiplicité de la fibre spéciale définie en 7.2.1.2.

Dans l'article de Wittenberg, la preuve de cet énoncé renvoie à [27], au chapitre 9.1, corollaire 9 et lemme 4. Donnons une vague idée de pourquoi cet énoncé est vrai : si Z est une composante intègre de la fibre spéciale $\mathcal{X}_k$, on construit un point fermé de $\mathcal{X}$, $\gamma : \text{Spec}(\mathcal{O}_L) \longrightarrow \mathcal{X}$ avec L/K une extension finie, de sorte que γ traverse Z en un point x qui est dans une seule composante irréductible de $\mathcal{X}_k$. On a alors des morphismes d'anneaux locaux :

$$\mathcal{O}_{\mathcal{X},Z} \longrightarrow \mathcal{O}_{\mathcal{X}_x} \longrightarrow \mathcal{O}_L$$

qui permettent de comparer la valuation de π dans $\mathcal{O}_L$ à son ordre d'annulation dans $\mathcal{O}_{\mathcal{X},Z}$.

7.2.2 Apparté sur la résolution des singularités

Un autre ingrédient essentiel dans les dévissages faits par Wittenberg pour obtenir la propriété de transition (et plus tard pour obtenir que les corps de nombres totalement imaginaires sont C_1^1) est une forme de "résolution" des singularités, où l'on utilise des guillemets car en caractéristique non-nulle on est obligé d'utiliser une forme plus faible de résolution des singularités puisque celle-ci n'est pas prouvée.
Expliquons rapidement de quoi traite la résolution des singularités sur un corps K. L'idée générale de la résolution des singularités est de partir d'un K-schéma X disons de type fini séparé et de construire un schéma X' et un morphisme $X' \xrightarrow{f} X$ tels que :

— X et X' se ressemblent beaucoup, ce qui peut vouloir dire que f est propre, birationnelle, ou du moins qu'elle est finie, ou génériquement finie, et qu'on contrôle bien les degrés des extensions résiduelles en les points maximaux.

— X' est régulier.

Une première idée est de considérer la normalisation $\widetilde{X}$ de X, qui est bien birationnelle à X mais n'est régulier que sur le complémentaire d'un fermé de codimension au moins 2. Si X est une courbe, cela fournit donc bien une résolution des singularités.
En caractéristique 0, la résolution des singularités est entièrement résolue par Hironaka.

Théorème 7.2.2.1. *(Hironaka) Soit K un corps de caractéristique 0 et X un K-schéma de type fini séparé. Il existe alors $Y \longrightarrow X$ un morphisme propre et birationnel de K-schémas de type fini séparés avec Y régulier (et donc lisse sur K car K est parfait).*

La preuve originale d'Hironaka est très compliquée et repose sur l'idée d'éclater X en des sous-variétés régulières pour faire baisser certains invariants numériques jusqu'à avoir résolu le problème. Elle a depuis été reformulée et grandement simplifiée.
Pour ce qui est de la caractéristique positive, le résultat n'est pas connu à ce jour mais De Jong a proposé une alternative dans son article [11]. Il introduit le concept plus faible d'altération et démontre que X possède toujours une altération régulière.

Définition 7.2.2.2. *Soit X un K-schéma de type fini séparé. Une altération de X est un K-schéma de type fini séparé Y de même dimension que X muni d'un morphisme $Y \longrightarrow X$ propre et dominant.*

Les résultats de De Jong ont ensuite été raffinés par Gabber (voir la présentation d'Illusie [8] à ce sujet) pour s'appliquer à des situations plus générales. Les deux résultats qu'on utilisera sont adaptés de [8], théorème 1.4 et [11], théorème 5.9, et sont présentés ici dans la forme plus simple dont on aura besoin.

Théorème 7.2.2.3. *(Gabber)*
Soit R un anneau de valuation discrète complet de corps résiduel k et de corps des fractions K et soit $\mathcal{X}$ un schéma propre sur R, irréductible pour simplifier. Soit ℓ un nombre premier non-nul dans k. Il existe alors une altération $Y \longrightarrow X$ génériquement finie, de degré en le point générique premier à ℓ, induite par un morphisme $\mathcal{Y} \longrightarrow \mathcal{X}$ de R-schémas, avec $\mathcal{Y}$ régulier propre et plat sur R.

Le théorème suivant affirme qu'en général, on peut modifier un schéma $\mathcal{X}$ en un schéma qui n'est pas tout à fait régulier mais qui possède seulement des singularités quotients, avec cette fois-ci un morphisme birationnel propre entre les deux.

Théorème 7.2.2.4. *(Version équivariante du théorème de Gabber)*
Soit R un anneau de valuation discrète complet de corps résiduel k et de corps des fractions K et soit $\mathcal{X}$ un schéma propre irréductible sur R. Il existe alors un R-schéma $\mathcal{Y}$ irréductible, régulier, projectif et plat muni d'une action R-linéaire d'un groupe fini G et un morphisme $f : \mathcal{Y}/G \longrightarrow \mathcal{X}$ propre et birationnel.

7.2.3 Preuve du théorème de transition de Wittenberg

On démontre alors le théorème 7.2.0.2 en gardant les notations du théorème.
Toutes les hypothèses restant vraies en passant à une extension finie, il suffit de montrer que pour tout K-schéma propre X et tout faisceau cohérent $\mathcal{F}$ sur X, $\chi(X, \mathcal{F})$ annule la ℓ^∞-torsion de $K_q(K)/N_q(X/K)$.
On utilise alors un dévissage à la Wittenberg 5.2.0.2 portant sur l'entier n_X défini comme la plus

grande puissance de ℓ qui divise l'exposant de $K_q(K)/N_q(X/K)$ si X est non-vide, et 0 sinon.
La divisibilité entre les entiers n_X n'est pas difficile à établir, et on doit donc trouver, pour tout K-schéma propre intègre X, un schéma intègre propre Y au dessus de X pour lequel $n_Y \mid \chi(Y)$, dont le degré au dessus de X est premier à ℓ.
Par le théorème de Gabber 7.2.2.3, on trouve un schéma Y au dessus de X propre et intègre, dont le degré au dessus de X est premier à ℓ, sous la forme $Y = \mathcal{Y}_K$ avec $\mathcal{Y}$ un R-schéma irréductible, régulier, propre et plat.
On se ramène donc à l'énoncé suivant.

Lemme 7.2.3.1. *Sous les hypothèses et notations du théorème précédent, si $\mathcal{X}$ est un R-schéma irréductible, régulier, propre et plat, et si $X = \mathcal{X}_K$, alors on a $n_X \mid \chi(X)$.*

Donnons les ingrédients principaux de la preuve de cet énoncé. L'idée est de se ramener à la fibre spéciale de X, qui est un k-schéma propre, puis d'utiliser l'hypothèse sur le corps k.

Démonstration. On note μ la multiplicité de la fibre spéciale de $\mathcal{X}$, définie en 7.2.1.2. Ainsi, le diviseur associé à une uniformisante π de R s'écrit μD avec D un diviseur effectif contenu dans la fibre spéciale. À D, on associe un fermé Z défini par le faisceau d'idéaux $\mathcal{O}_{\mathcal{X}}(-D)$.
Puisque Z est un k-schéma propre et par hypothèse sur le corps k, on obtient que $\chi(Z)$ annule la ℓ^∞-torsion du groupe $K_{q-1}(k)/N_{q-1}(Z/k)$, mais ce groupe est aussi égal à $K_{q-1}(k)/N_{q-1}(\mathcal{X}_k/k)$ car les points fermés de Z et de $\mathcal{X}_k$ sont les mêmes : ces deux schémas ont le même sous-schéma réduit.
On utilise alors le corollaire 7.2.1.5 qui affirme que :

$$N_{q-1}(\mathcal{X}_k/k) = \partial N_q(\mathcal{X}_K/K)$$

et donc que $\chi(Z)$ annule la ℓ^∞-torsion de $K_{q-1}(k)/\partial N_q(\mathcal{X}_K/K)$.
Ainsi, dans la suite exacte 7, avec $X = \mathcal{X}_K$:

$$0 \longrightarrow \frac{U_q(K)}{U_q(K) \cap N_q(X/K)} \longrightarrow \frac{K_q(K)}{N_q(X/K)} \longrightarrow \frac{K_{q-1}(k)}{\partial N_q(X/K)} \longrightarrow 0$$

$\chi(Z)$ tue la ℓ^∞-torsion du membre de droite. Ensault, Levine et Wittenberg démontrent dans [7], proposition 2.4, que $\chi(X) = \mu\chi(Z)$ de sorte que si l'on montre aussi que μ tue la ℓ^∞-torsion du membre de gauche que l'on note G, on aura gagné. Par la proposition 7.2.1.7, il suffit en fait de montrer que l'indice de ramification $[\mathcal{X} : K]_{\text{ram}}$ tue la ℓ^∞-torsion de G.
Autrement dit, il suffit de montrer que pour toute extension finie M/K où $\mathcal{X}$ possède un point, l'indice de ramification $e(M/K)$ de l'extension M/K tue la ℓ^∞-torsion de G.
On s'attaque donc à ce dernier point. Pour cela, on contemple, avec les notations de 4, le diagramme commutatif à lignes exactes suivant (voir le troisième point de la proposition 4.3.0.2) en notant m le corps résiduel de M :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_q^1(M) & \longrightarrow & U_q(M) & \longrightarrow & K_q(m) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle N_{M/K}} & & \downarrow{\scriptstyle N_{M/K}} & & \downarrow{\scriptstyle e(M/K)N_{m/k}} & & \\
0 & \longrightarrow & U_q^1(K) & \longrightarrow & U_q(K) & \longrightarrow & K_q(k) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \dfrac{U_q^1(K)}{N_{M/K}U_q^1(M)} & \longrightarrow & \dfrac{U_q(K)}{N_{M/K}U_q(M)} & \longrightarrow & \dfrac{K_q(k)}{e(M/K)N_{m/k}K_q(m)} & \longrightarrow & 0
\end{array}$$

avec la troisième ligne qui s'obtient en prenant les conoyaux. Observons que $U_q^1(K)$ est ℓ-divisible parce que $1+\mathfrak{m}_K$ l'est par complétude de K et parce que ℓ est différent de la caractéristique résiduelle, de sorte que le quotient $U_q^1(K)/N_{M/K}U_q^1(M)$ est ℓ-divisible et de torsion et donc que son produit tensoriel avec $\mathbb{Z}_\ell$ est nul.
On tensorise alors la troisième ligne par $\mathbb{Z}_\ell$ et on obtient un isomorphisme :

$$\frac{U_q(K)}{N_{M/K}U_q(M)} \otimes \mathbb{Z}_\ell \cong \frac{K_q(k)}{e(M/K)N_{m/k}K_q(m)} \otimes \mathbb{Z}_\ell.$$

Comme k vérifie C_0^q en ℓ, le deuxième membre de cet isomorphisme est tué par $e(M/K)$ et donc le premier aussi. Ceci conclut la preuve de ce lemme, et du théorème de Wittenberg 7.2.0.2. □

Chapitre 8

Propriétés diophantiennes des corps p-adiques

Le but de cette partie est de comprendre la preuve de Wittenberg du fait que les corps p-adiques vérifient la propriété C_1^1 de Kato et Kuzumaki, confirmant ainsi la conjecture de Kato et Kuzumaki pour ces corps-ci car ils sont de dimension cohomologique 2 d'après le corollaire 7.1.0.5 (qui reste vrai si le corps résiduel est de caractéristique positive). Rappelons qu'on a vu, dans le théorème 7.2.0.2 de Wittenberg qu'un corps p-adique vérifie toujours la propriété C_1^1 forte en dehors de p.
On sera naturellement amenés, dans cette partie, à s'intéresser aux schémas sur des anneaux de valuation discrète et sur des corps finis. On fera donc appel aux bornes de Lang-Weil-Nisnevič qui interviennent dans les questions de points rationnels sur les corps finis.

8.1 Bornes de Lang-Weil-Nisnevič

Les bornes de Lang-Weil-Nisnevič sont aujourd'hui un corollaire des conjectures de Weil, mais elles peuvent aussi se démontrer directement [26]. On utilisera dans la suite la forme suivante :

Théorème 8.1.0.1. *(Bornes de Lang-Weil-Nisnevič) Soit k un corps fini de cardinal q et X un k-schéma de type fini géométriquement irréductible séparé de dimension $d \geq 1$. Il existe alors une constante $C > 0$ telle que, pour toute extension finie ℓ/k :*

$$\left|X(\ell) - |\ell|^d\right| \leq C\,|\ell|^{d-\frac{1}{2}}.$$

En particulier, X a des points dans $\mathbb{F}_{q^n}$ pour n assez grand, et pour tout $m \geq 1$, X possède un point dans une extension de k de degré premier à m. Ceci implique aussi que :

$$[X : k] = 1.$$

Dans le cas où X n'est pas géométriquement irréductible, on a quand même l'énoncé suivant.

Corollaire 8.1.0.2. *Soit k un corps fini de cardinal q et X un k-schéma de type fini séparé. On a alors :*

$$[X : k]_{\text{ét}} = [X : k] = [X : k]_{\chi}$$

avec $[X : k]_{\text{ét}}$ l'indice étendu défini comme le pgcd *des degrés des extensions k_Z avec Z composante intègre de X (k_Z désigne la clôture algébrique de k dans $k(Z)$), et $[X : k]_{\chi}$ l'indice cohomologique (voir 5.2.0.1).*

Démonstration. On rappelle qu'on a toujours $[X:k]_{\text{ét}} \mid [X:k]_\chi \mid [X:k]$.
Soit maintenant Z une composante intègre de X et $\ell = k_Z$ son corps des constantes. L'extension ℓ/k est finie car ℓ est une extension algébrique et de type finie car contenue dans une extension de type fini $k(Z)/k$. Montrons que toute composante intègre W de Z_ℓ est géométriquement intègre : ceci n'est pas automatique et repose sur le caractère fini de k (par exemple, si X est le schéma $X^3 = 2$ sur le corps $\mathbb{Q}$, il est intègre, son corps des constantes est $L = \mathbb{Q}(\alpha)$ avec $\alpha = 2^{1/3}$ et X_L est formé de deux composantes intègres dont une qui n'est pas géométriquement intègre car son changement de base à la clôture galoisienne de L n'est pas intègre).
Tout repose sur le fait que ℓ/k est galoisienne, de sorte que $G = \mathrm{Gal}(\ell/k)$ agit sur les composantes intègres de Z_ℓ. Le point générique de Z donne un morphisme dominant :

$$\operatorname{Spec} k(Z) \longrightarrow Z$$

qui par platitude de ℓ/k donne encore un morphisme dominant :

$$\operatorname{Spec} k(Z) \otimes_k \ell \longrightarrow Z_\ell.$$

Or on a :

$$k(Z) \otimes_k \ell = k(Z) \otimes_\ell (\ell \otimes_k \ell) = k(Z) \otimes_\ell \prod_{\sigma \in G} \ell = \prod_{\sigma \in G} k(Z)$$

de sorte qu'on a un morphisme dominant et G-équivariant :

$$\bigsqcup_{\sigma \in G} \operatorname{Spec} k(Z) \xrightarrow{f} Z_\ell.$$

Notons η_σ le point de $\operatorname{Spec} k(Z)$ dans la copie indexée par σ. À cause de l'action de G qui est transitive sur les η_σ, les fermés irréductibles $\overline{f(\eta_\sigma)}$ ont tous la même dimension, et comme f est dominante, ce sont des composantes irréductibles de Z_ℓ. Ainsi, les composantes irréductibles de Z_ℓ ont toutes même dimension et G agit transitivement dessus. Ainsi, si $W = \overline{f(\eta_\sigma)}$ est une composante irréductible (réduite) de Z_ℓ, et si U est un ouvert affine dense de W, on a un morphisme injectif d'anneaux :

$$\mathcal{O}(U) \longrightarrow k(Z)$$

et comme U est un ℓ-schéma, on a aussi $\ell \subseteq \mathcal{O}(U) \subseteq k(Z)$, or ℓ est algébriquement clos dans $k(Z)$ par construction, donc dans $\mathrm{Frac}(\mathcal{O}(U))$, ce qui montre bien que W est géométriquement intègre.

Ainsi les bornes de Lang-Weil Nisnevič assurent que W possède un 0-cycle de degré 1, de sorte que Z possède un 0-cycle de degré $[k_Z : k]$. On a donc :

$$[X:k] \mid [k_Z : k]$$

ce qui permet de conclure. □

8.2 Les corps p-adiques sont C_1^1

Nous avons tous les ingrédients en main pour comprendre la preuve de Wittenberg du fait que les corps p-adiques sont C_1^1. L'idée est d'utiliser un dévissage grâce aux altérations de De Jong, en se basant sur la réflexion suivante : si X est un schéma de type fini non-vide sur un corps p-adique K

de corps résiduel k, l'indice résiduel $[X:K]_{\text{res}}$ défini plus haut comme le pgcd des degrés d'inertie des extensions de K où X possède un point est égal à l'ordre du groupe cyclique :

$$K_0(k)/\partial N_1(X/K)$$

car $K_0(k) = \mathbb{Z}$ et ∂ est donné par la valuation. On utilisera alors la suite exacte 7 pour conclure.
En dévissant grâce au théorème 5.2.0.2 de Wittenberg, on obtient que pour tout K-schéma propre X et tout faisceau cohérent $\mathcal{F}$ sur X, on a :

$$[X:K]_{\text{res}} \mid [X:K]_{\chi}.$$

Démonstration. En effet, il faut vérifier que pour tout K-schéma propre X intègre, il existe $f : Y \longrightarrow X$ birationnel avec Y propre et intègre sur K tel que $[Y:K]_{\text{res}} \mid \chi(Y)$.
En considérant K_X le corps des constantes de X qui est une extension finie de X et X' la normalisation de X, qui est naturellement un K_X-schéma géométriquement intègre et propre, et en appliquant le theorème 7.2.2.4 à un modèle propre de X' sur l'anneau des entiers $\mathcal{O}_{K_X}$, on se ramène à montrer que si $\mathcal{Y}$ est un schéma irréductible, régulier, projectif et plat sur l'anneau des entiers R de K sur lequel un groupe fini G agit de façon R-linéaire, et si l'on pose $\mathcal{X} = \mathcal{Y}/G$, alors :

$$[\mathcal{X}:K]_{\text{res}} \mid \chi(\mathcal{X}_K).$$

On utilise alors la seconde partie de la proposition 7.2.1.4 pour obtenir :

$$[\mathcal{X}:K]_{\text{res}} = [\mathcal{X}_k : k].$$

La platitude de $\mathcal{X}$ sur R entraîne alors que :

$$\chi(\mathcal{X}_K) = \chi(\mathcal{X}_k)$$

et ainsi on se ramène à montrer la divisibilité suivante :

$$[\mathcal{X}_k : k] \mid \chi(\mathcal{X}_k).$$

Les corollaires 5.2.0.3 et 8.1.0.2 permettent de conclure. □

On en déduit finalement le théorème suivant.

Théorème 8.2.0.1. *(Wittenberg)*
Les corps p-adiques vérifient la propriété C_1^1.

Démonstration. Une extension finie d'un corps p-adique est encore un corps p-adique, donc il s'agit simplement de montrer que si K est un corps p-adique et X une hypersurface de $\mathbb{P}^n$ de degré $d \leq n$, alors on a :

$$K^\times = N_1(X/K).$$

De ce qui précède, on a :

$$[X:K]_{\text{res}} = 1$$

car $\chi(X) = 1$. On en déduit :

$$K_0(k)/\partial N_1(X/K) = 0$$

et la suite exacte 7 pour $q = 1$ donne alors un isomorphisme :

$$\frac{R^\times}{R^\times \cap N_1(X/K)} \cong \frac{K^\times}{N_1(X/K)}.$$

L'extension maximale non-ramifiée de K, K^{nr}, est un corps C^1 par le théorème de Lang 6.1.0.10 et la remarque 6.1.0.11 donc X possède un point dans une extension L/K finie non-ramifiée, et la norme $\mathcal{O}_L^\times \longrightarrow R^\times$ est surjective, donc le terme de gauche de l'isomorphisme est nul, ce qui permet de conclure. □

Chapitre 9

La propriété C_1^1 pour les corps de nombres

On s'intéresse à présent à la conjecture de Kato et Kuzumaki pour les corps de nombres. Le seul cas intéressant est celui des corps de nombres totalement imaginaires, qui sont de dimension cohomologique 2, sinon la dimension cohomologique est infinie et la propriété C_i^q n'est jamais vérifiée.
On présente ici deux preuves différentes du théorème suivant, l'une due à Izquierdo et l'autre à Wittenberg, dans l'ordre anti-chronologique.

Théorème 9.0.0.1. *Tout corps de nombres totalement imaginaire est C_1^1.*

Les deux sont basées sur le cas des corps p-adiques établi par Wittenberg et sur un principe local global. La preuve d'Izquierdo repose aussi sur la théorie des corps hilbertiens et est assez directe une fois qu'on a mis en place la théorie des tores multinormiques, tandis que celle de Wittenberg passe par un dévissage qui provient encore une fois du théorème 5.2.0.2. On présente les deux approches dans la suite.
Dans les deux cas notons que, comme toute extension finie d'un corps de nombres totalement imaginaire est encore totalement imaginaire, il suffit de montrer que pour toute hypersurface X de $\mathbb{P}^n_K$ de degré au plus n, on a :

$$H(X/K) = 0$$

avec $H(X/K) = \frac{K^\times}{N_1(X/K)}$. Commençons par établir quelques notations et définitions.

Définition 9.0.0.2. *Soit K un corps de nombres et X un K-schéma de type fini. On lui associe un système d'extensions de K, $\mathcal{L}_X$ défini comme l'ensemble des extensions finies de K sur lesquelles X possède un point. Suivant la définition 3.6.0.1, on définit le tore multinormique infini T_X via la formule suivante :*

$$T_X = T_{\mathcal{L}_X}.$$

On a alors clairement, pour toute extension finie E/K :

$$T_{X\times_K E} = T_{\mathcal{L}_X^E}.$$

Ceci permet de définir les groupes de cohomologie $H^1(K, T_X)$ et de Tate-Shafarevich $Ш^1(K, T_X)$. On a alors :

$$H(X/K) = H^1(K, T_X).$$

Enfin, notons que si S est un ensemble quelconque de places de K, il est possible de définir des groupes de Tate-Shafarevich restreints aux places de S :

$$Ш^n_S(K, A) = \mathrm{Ker}\left(H^n(K, A) \longrightarrow \prod_{v\in S} H^n(K_v, A)\right)$$

pour A un G_K-module topologique.

9.1 Approche de D. Izquierdo par la théorie des corps hilbertiens

L'idée de la preuve d'Izquierdo est la suivante. On sait que chaque $H(X_v/K_v)$ est nul d'après le cas des corps p-adiques 8.2.0.1 et parce que K est totalement imaginaire. Il reste alors à montrer que le morphisme :

$$H(X/K) \longrightarrow \prod_{v\in\Omega_K} H(X_v/K_v)$$

est injectif. Pour cela, on commence par faire l'observation suivante, très naturelle, qui justifie l'utilisation des groupes de Tate-Shafarevich pour résoudre ce problème. La preuve de ce lemme repose sur le théorème de Greenberg et sur le théorème de Tarski-Seidenberg si on veut autoriser des places réelles.

Lemme 9.1.0.1. *Soit K un corps de nombres et X un K-schéma. On a alors l'égalité suivante :*

$$Ш^1(K,T_X) = \mathrm{Ker}\left(H(X/K) \longrightarrow \prod_{v\in\Omega_K} H(X_v/K_v)\right).$$

Démonstration. Il s'agit de montrer que si $[x] \in H(X/K)$ avec $x \in K^\times$, alors pour toute place v les énoncés suivants sont équivalents :

— x est un élément de $N_1(X_v/K_v)$.

— x est dans $\langle N(L_v/K_v) \mid X(L) \neq \emptyset\rangle$.

Le second point implique bien le premier car L_v se scinde en un produit d'extensions finies de K_v qui contiennent L, de sorte que X a bien des points sur chacune d'elles. Ensuite, en supposant que $x = N_{\mathfrak{L}/K_v}(y)$ avec $\mathfrak{L}$ une extension finie de K_v telle que $X(\mathfrak{L}) \neq \emptyset$, montrons le second point. On peut clairement supposer X affine, et on note $\mathfrak{L}'$ la clôture algébrique de K dans $\mathfrak{L}$.
Si v est finie, il est alors possible de trouver un modèle $\mathcal{X}$ de X sur l'anneau de valuation discrète $\mathcal{O}_{K_v}$ qui possède un $\mathcal{O}_{\mathfrak{L}}$-point.
Ainsi, $\mathcal{X}$ possède un $\mathcal{O}_{\mathfrak{L}}/\mathfrak{m}_{\mathfrak{L}}^n$-point pour tout n, et par le théorème d'approximation de Greenberg 6.1.0.9, comme l'anneau $\mathcal{O}_{\mathfrak{L}} \cap \mathfrak{L}'$ est hensélien excellent, $\mathcal{X}$ possède un point dans cet anneau donc dans $\mathfrak{L}'$, et donc X aussi. Ainsi X possède un point dans une extension finie L de K telle que $L \subseteq \mathfrak{L}$, ce qui permet de conclure.
Si v est complexe, ce qu'on veut montrer découle directement du Nullstellensatz.
Le cas réel repose sur l'utilisation du principe de Tarski-Seidenberg (corollaire 4.1.6 de [21]) : il s'agit de montrer que si K est un corps de nombres contenu dans $\mathbb{R}$ et si X a un point réel, alors X a un point sur la clôture algébrique de K dans $\mathbb{R}$. Puisqu'on ne s'intéresse dans cette partie qu'au cas des corps de nombres totalement imaginaires, ce point n'est d'ailleurs pas très important. □

On s'intéresse à présent à un cas où ce groupe de Tate-Shafarevich est nul. C'est une application du théorème de Demarche et Wei généralisé 3.6.0.5.

Théorème 9.1.0.2. *(Izquierdo)*
Soit K un corps de nombres et X un K-schéma de type fini qui contient un fermé géométriquement intègre. Le système d'extensions $\mathcal{L}_X$ est alors séparé (voir définition 3.6.0.2) et en particulier :

$$Ш^1(K,T_X) = 0.$$

Démonstration. Il suffit de montrer que $\mathcal{L}_X$ est séparé puis d'appliquer le théorème d'annulation de Demarche et Wei généralisé 3.6.0.5. En d'autres termes, il s'agit de montrer que si X a un point dans une extension finie L/K, alors il existe L' où X a aussi un point avec $L' \cap L = K$.
Au vu des hypothèses, on peut ici supposer que X est géométriquement intègre et affine, quitte à oublier le fait que X a un point dans L : ça n'est même pas nécessaire à la preuve. Par un théorème de Bertini appliqué à un ouvert affine de X, X contient une courbe quasi-projective géométriquement intègre, et ainsi on peut supposer que X est une courbe quasi-projective géométriquement intègre. On peut même supposer, quitte à prendre un ouvert plus petit, que cette courbe est contenue dans $\mathbb{P}^2_K$ car elle est birationnelle à une courbe plane. Ainsi, X est un ouvert d'une courbe projective plane C définie par l'équation $g(X,Y,Z) = 0$ avec g irréductible homogène, qu'on peut supposer dépendant non-trivialement de la première variable, i.e. $\partial_X g \neq 0$.
Par la théorie des corps *Hilbertiens* (voir l'article d'Izquierdo [10] pour les détails) et puisque g est irréductible sur K, il existe une infinité de couples $(y,z) \in K^2$ tels que le polynôme $g(X,y,z)$ est irréductible sur L. Puisque X est cofini dans la courbe C, on a donc une infinité de points fermés $[x : y : z]$ de X avec $y,z \in K$ tels que, si $L' = K(x)$, alors $L' \cap L = K$ car L' est le corps de rupture de $g(X,y,z)$, irréductible sur L. □

Voici comment déduire de ce théorème la preuve du fait que les corps de nombres totalement imaginaires vérifient la propriété C_1^1.

Démonstration. Soit donc K un corps de nombres totalement imaginaire et X une hypersurface de $\mathbb{P}^n_K$ de degré au plus n. On a ainsi :

$$\chi(X) = 1.$$

Or, par le corollaire 5.2.0.3 du principe de dévissage à la Wittenberg, l'indice étendu de X sur K divise $\chi(X)$, et donc vaut 1. On en déduit qu'il existe des fermés intègres $Z_1, \dots, Z_r$ de X tels que, en notant K_i la clôture algébrique de K dans $K(Z_i)$, on ait :

$$\mathrm{pgcd}_i [K_i : K] = 1.$$

Ainsi, pour tout i, X_{K_i} possède un fermé géométriquement intègre : il suffit de prendre une composante irréductible de $(Z_i)_{K_i}$, qui est géométriquement irréductible car K_i est algébriquement clos dans son corps des fonctions, et il est géométriquement réduit car il est réduit et K est de caractéristique nulle.
On applique alors le théorème 9.1.0.2 :

$$Ш^1(K_i, T_{X_{K_i}}) = 0$$

pour tout i, avec la notation du théorème 9.1.0.2.
Un principe de restriction-corestriction (voir 3.6) permet d'en déduire que pour tout i, $[K_i : K]$ tue le groupe $Ш^1(K, T_X)$ et donc que ce groupe est nul. On en déduit le théorème 9.0.0.1 par le cas connu des corps p-adiques 8.2.0.1. □

9.2 Approche de O. Wittenberg par dévissage

L'idée de la preuve de Wittenberg est d'utiliser le dévissage 5.2.0.2 démontré dans l'apparté géométrique pour se ramener aux cas des variétés lisses de caractéristique d'Euler 1, sur lesquelles l'énoncé s'obtient par passage local global et par la formule de Riemann-Roch-Hirzebruch. Les ingrédients pour justifier ce passage local global viennent de l'article de Kato et Saito [13]. On les résume dans le lemme suivant dont on ne donnera pas de preuve.

Lemme 9.2.0.1. *(Kato, Saito) Soit K un corps de nombres et X une variété propre lisse géométriquement irréductible sur K. Le morphisme :*

$$N_1(X/K) \longrightarrow \prod_{v\in S} N_1(X_v, K_v)$$

est alors d'image dense. De plus, si S est un ensemble fini de places de K, on a :

$$Ш^1_S(K, T_X) \cong \prod_{v\notin S} H(X_v/K_v).$$

On peut à présent expliquer la preuve de Wittenberg du théorème 9.0.0.1.

Démonstration. Fixons $n \geq 1$.
Si X est un schéma propre non-vide sur un corps K, on note $[X : K]$ l'indice de X sur K, c'est à dire le pgcd des degrés des corps résiduels de X sur K (qui vaut 0 si X est vide). On a alors $[X : K]H(X/K) = 0$ et donc $H(X/K)$ est toujours un groupe de torsion.
Notre but est toujours de montrer que si K est totalement imaginaire et X est une hypersurface de $\mathbb{P}^n_K$ de degré $d \leq n$, alors $H(X/K) = 0$.
On considère alors S l'ensemble des places finies de K de caractéristique résiduelle inférieure ou égale à N, un entier qui ne dépend que de n à choisir plus tard, et on s'intéresse, pour tout schéma propre sur K au groupe de Tate-Shafarevich restreint du tore multinormique associé à X :

$$Ш^1_S(K, T_X) = \mathrm{Ker}\left(H(X/K) \longrightarrow \prod_{v\in S} H(X_v/K_v)\right).$$

Cette égalité vient du lemme 9.1.0.1 dont la preuve s'adapte tout à fait au cas restreint.
Remarquons ensuite que, si X est non-vide, le groupe $N_1(X_v/k_v)$ est un sous-groupe ouvert de $K_v^\times$ car il contient $(K_v^\times)^{[X:k_v]}$.
On considère alors n_X l'exposant du groupe $Ш^1_S(K, T_X)$ si X est non-vide, et $n_X = 0$ sinon. On a ainsi $n_X \mid [X : K]$. On va lui appliquer le principe de dévissage 5.2.0.2 pour voir que $n_X \mid \chi(X)$. Ceci permettra de conclure car, dans le cas qui nous intéresse, X est une hypersurface de degré inférieur ou égal à n et donc $\chi(X) = 1$, et on aura donc $H(X/K)$ qui s'injecte dans $\prod_{v\in S} H(X_v/K_v)$, mais ce groupe-ci est nul parce que K_v vérifie la propriété C_1^1 d'après 8.2.0.1. Vérifions donc que le dévissage s'applique bien pour les K-schémas propres de dimension au plus $n-1$.
D'abord, si $f : Y \longrightarrow X$ est un morphisme de K-schémas propres non-vides, on a un morphisme induit :

$$H(Y/K) \longrightarrow H(X/K)$$

et de même au niveau des complétés, ce qui donne un morphisme :

$$Ш^1_S(K, T_Y) \longrightarrow Ш^1_S(K, T_X).$$

Montrons que ce morphisme est surjectif, ce qui nous donnera :

$$n_X \mid n_Y.$$

Soit donc $[x] \in Ш^1_S(K, T_X)$, avec $x \in K^\times$. Pour tout $v \in S$, on a $x \in N_1(X_v/K_v)$, or par 9.2.0.1, l'application $N_1(X/K) \longrightarrow \prod_{v\in S} N_1(X_v, K_v)$ est d'image dense de sorte qu'on peut supposer x_v aussi proche de 1 qu'on veut pour tout $v \in S$ sans changer $[x]$, et en particulier $x_v \in N_1(Y_v, k_v)$ car c'est un sous-groupe

ouvert (Y étant non-vide), et ainsi $[x]$ vient d'un élément de $Ш^1_S(K, T_X)$.
Ensuite, si X est un schéma propre intègre sur K (donc non-vide) de dimension au plus $n-1$, comme on est en caractéristique 0, la résolution des singularités d'Hironaka 7.2.2.1 s'applique et on obtient un schéma propre intègre *lisse* Y et un morphisme birationnel $Y \longrightarrow X$, donc de degré 1 qui est premier à n_X, et il reste à vérifier que :

$$n_Y \mid \chi(Y)$$

pour terminer la preuve du dévissage à la Wittenberg. Pour pouvoir appliquer la deuxième partie du lemme 9.2.0.1 de Kato et Saito, on a besoin de se ramener au cas où Y est *géométriquement intègre*. Y est déjà géométriquement réduit car on est en caractéristique 0, et si l'on note K_Y la clôture algébrique de K dans $K(Y)$, Y est un schéma géométriquement intègre sur K_Y car il est normal (on note Y' ce schéma sur K_Y) et on a un morphisme donné par la norme de K_Y sur K :

$$Ш^1_{S'}(K_Y, T_{Y'}) \longrightarrow Ш^1_S(K, T_Y)$$

avec S' l'ensemble des places de K_Y au dessus de K (K_Y/K est une extension finie car elle est algébrique et c'est une sous-extension d'une extension finiment engendrée).
Le conoyau de ce morphisme est annulé par $[K_Y : K]$ car si $[x] \in Ш^1_S(K, T_Y)$, on a $x^{[K_Y:K]} = N_{K_Y/K}(x)$ et on peut supposer que la classe de x dans $H(Y'/K_Y)$ soit dans $Ш^1_{S'}(K_Y, T_{Y'})$ quitte à rapprocher x de 1 en chaque place en utilisant le même argument de densité qu'avant.
On en déduit que $n_Y \mid n_{Y'}[K_Y : K]$.
De plus :

$$\chi(Y) = \sum_i (-1)^i \dim_K H^i(Y, \mathcal{O}_Y) = \sum_i (-1)^i [K_Y : K] \dim_{K_Y} H^i(Y, \mathcal{O}_Y) = [K_Y : K]\chi(Y')$$

de sorte que, si on sait que $n_{Y'} \mid \chi(Y')$, on obtient $n_Y \mid \chi(Y)$.
Il reste donc à démontrer que, si X est une variété projective lisse géométriquement intègre sur K de dimension au plus $n-1$, on a $n_X \mid \chi(X)$.
Or, X étant lisse, le corollaire de la formule de Riemann-Roch-Hirzebruch 5.4.0.6 donne :

$$n_X \mid [X : K] \mid \chi(X)$$

dans l'anneau $\mathbb{Z}[1/(2(n-1))!]$, autrement dit la divisibilité $n_X \mid \chi(X)$ vaut en tout nombre premier suffisament grand, disons plus grand que N qui ne dépend que de n.
Mais la seconde partie du lemme de Kato et Saito 9.2.0.1 donne un isomorphisme canonique :

$$Ш^1_S(K, T_X) \cong \prod_{v \notin S} H(X_v/K_v).$$

Soit donc v une place qui n'est pas dans S. Si v est complexe, le groupe $H(X_v/k_v)$ est nul. Sinon, v est finie de caractéristique $p > N$ car K est *totalement imaginaire*.
Puisque K_v vérifie la propriété C_1^1 forte *en dehors de p* par 7.2.0.2, on a :

$$\exp(H(X_v/k_v)) \mid \chi(X_v) = \chi(X)$$

dans $\mathbb{Z}[1/p]$, avec $\exp(G)$ la notation pour l'exposant d'un groupe G.
On en déduit que la divisibilité $n_X \mid \chi(X)$ vaut en tout nombre premier p strictement plus petit que N, et donc au total on a bien montré $n_X \mid \chi(X)$, ce qui conclut la preuve de Wittenberg. □

Bibliographie

[1] Jean-Pierre Serre Armand Borel. Le théorème de riemann-roch. *Bulletin de la Société Mathétmatique de France*, 1958.

[2] Dasheng Wei Cyril Demarche. Hasse principle and weak approximation for multinorm equations, 2013. URL : https://arxiv.org/abs/1212.5889, arXiv:1212.5889.

[3] Joe Harris David Eisenbud. *Intersection Theory in Algebraic Geometry*.

[4] Tamás Szamuely David Harari. Arithmetic duality theorems for 1-motives, 2004. URL : https://arxiv.org/abs/math/0304480, arXiv:math/0304480.

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

[6] Marvin Jay Greenberg. Rational points in henselian discrete valuation rings. *Publications mathéatiques de l'I.H.É.S.*, 1966.

[7] Olivier Wittenberg Hélène Esnault, Marc Levine. Index of varieties over henselian fields and euler characteristic of coherent sheaves. *Journal of Algebraic Geometry*, 2015. URL : http://dx.doi.org/10.1090/jag/639.

[8] Luc Illusie. On gabber's refined uniformization. 2008.

[9] Diego Izquierdo. Le théorème de poitou-tate à partir du théorème d'artin-verdier, 2013.

[10] 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.

[11] Aise J. De Jong. Families of curves and alterations. 1997.

[12] Bruno Kahn. La conjecture de milnor d'après v. voevodsky. *Séminaire Bourbaki*, (834), 1996-1997.

[13] Shuji Saito Kazuya Kato. Unramified class field theory of arithmetical surfaces. *Annals of Mathematics*, 1983.

[14] 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.

[15] Franz-Victor Khulmann. Book on valuation theory, chapter 24. URL : https://www.fvkuhlmann.de/bookch24.pdf.

[16] Tsit-Yuen Lam. *Introduction to Qadratic Forms over Fields*. 1973.

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

[18] James S. Milne. Algebraic groups. URL : https://www.jmilne.org/math/CourseNotes/iAG200.pdf.

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

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

[21] Alena Pirutka. Deux contributions à l'arithmétique des variétés : R-équivalence et cohomologie non ramifiée, 2011.

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

[23] Karen E. Smith Rankeya Datta. Frobenius and valuation rings. 2016. URL : https://par.nsf.gov/servlets/purl/10120922.

[24] Tsit-Yuen Lam Richard Elman. Pfister forms and k-theory of fields. 1972.

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

[26] André Weil Serge Lang. Number of points of varieties in finite fields. 1954.

[27] Michel Raynaud Siegfried Bosch, Werner Lütkebohmert. *Néron Models*. 1990.

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

[29] Vladimir Voevodsky. The milnor conjecture. 1996. URL : https://www.researchgate.net/publication/2426765_The_Milnor_Conjecture.

[30] 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.