Le Théorème de Poitou-Tate

Introduction au domaine de recherche

Diego IZQUIERDO
Sous la direction de David HARARI

Septembre 2013

Table des matières

Avertissement : Ce texte est une présentation générale d'un domaine. La compréhension globale nécessite peu de prérequis, le niveau M1 étant suffisant. Par contre, certaines preuves, que nous avons signalées avec une étoile, nécessitent plus de connaissances pour être comprises. Le lecteur s'initiant dans le domaine est donc invité à les sauter.

Dans toute la suite, pour chaque corps k, k^s désignera la clôture séparable de k et G_k le groupe de Galois absolu $\mathrm{Gal}(k^s/k)$ de k.

1 Introduction sur les corps de nombres et les corps p-adiques

1.1 Motivation

Au départ, la théorie des nombres s'intéresse aux propriétés de l'anneau $\mathbb{Z}$ et de son corps des fractions $\mathbb{Q}$. En particulier, la résolution d'équations polynomiales dans $\mathbb{Z}$ est au coeur de la théorie des nombres. Considérons donc $f \in \mathbb{Z}[X_1, ..., X_n]$ et demandons-nous si l'équation $f(X_1, ..., X_n) = 0$ possède des solutions dans $\mathbb{Z}$. En arithmétique élémentaire, quand on cherche à montrer qu'une telle équation n'a pas de solutions, on dispose en gros de deux méthodes très générales :

- prouver que l'équation n'a pas de solutions dans $\mathbb{R}$, ce qui revient à prouver une des deux inégalités $f(x_1, ..., x_n) < 0$ ou $f(x_1, ..., x_n) > 0$.
- trouver un entier naturel m tel que l'équation $f(x_1, ..., x_n) = 0$ n'a pas de solutions dans l'anneau $\mathbb{Z}/m\mathbb{Z}$. À l'aide du théorème des restes chinois, cela revient à trouver un nombre premier p et un entier naturel m tels que l'équation $f(x_1, ..., x_n) = 0$ n'a pas de solutions dans l'anneau $\mathbb{Z}/p^m\mathbb{Z}$.

Or, comme une limite projective d'ensembles finis non vides est non vide, si l'on fixe un nombre premier p, l'équation $f(X_1, ..., X_n) = 0$ a des solutions dans $\mathbb{Z}/p^m\mathbb{Z}$ pour tout $m > 0$ si, et seulement si, l'équation a une solution dans l'anneau $\mathbb{Z}_p = \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$, appelé **anneau des entiers p-adiques**. Par conséquent, les deux méthodes précédentes pour prouver que l'équation $f(X_1, ..., X_n) = 0$ n'a pas de solutions dans $\mathbb{Z}$ consistent à montrer que l'équation n'a pas de solutions dans $\mathbb{R}$ ou dans $\mathbb{Z}_p$ pour un certain p. Il est alors naturel de se demander s'il existe d'autres méthodes pour montrer que l'équation n'a pas de solutions dans $\mathbb{Z}$. Malheureusement, en général, il existe bien d'autres obstructions empêchant l'équation d'avoir des solutions. Cependant, pour certains types d'équations, les deux obstructions précédentes sont les seules :

Théorème 1.1.1. ***(Théorème de Hasse-Minkowski)***
Soit $f(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$ une forme quadratique. L'équation $f(x_1, ..., x_n) = 0$ a des solutions non nulles dans $\mathbb{Q}$ si, et seulement si, elle en a dans $\mathbb{R}$ et dans le corps des fractions $\mathbb{Q}_p$ de $\mathbb{Z}_p$ pour chaque premier p.

Remarque 1.1.2. La preuve de Minkowski n'a jamais été publiée. Hasse a prouvé une version plus générale du théorème (pour tous les corps de nombres et pas uniquement $\mathbb{Q}$) en 1921 dans sa thèse.

Démonstration. On pourra lire le théorème 8 du chapitre IV de [Ser77]. □

Un tel résultat, affirmant qu'une propriété est vraie sur $\mathbb{Q}$ si, et seulement si, elle l'est sur $\mathbb{R}$ et sur tous les $\mathbb{Q}_p$, relève de ce qu'on appelle **principe de Hasse**. Ce principe est particulièrement intéressant puisqu'il est nettement plus simple de travailler avec les corps $\mathbb{Q}_p$ qu'avec le corps $\mathbb{Q}$: en effet, le **lemme de Hensel**, un résultat fondamental sur les corps p-adiques, permet de construire une solution d'une équation dans $\mathbb{Z}_p$ à partir d'une solution de la même équation dans

$\mathbb{F}_p$. Il convient donc de disposer de moyens pour passer de $\mathbb{Q}$ aux corps $\mathbb{Q}_p$. Un de ces moyens est le **théorème de Poitou-Tate**.

1.2 Corps de nombres et corps p-adiques

Afin de mieux comprendre les corps $\mathbb{Q}_p$ et de les généraliser, il convient de les caractériser autrement. Fixons un nombre premier p. La formule $d_p(x,y) = p^{-v_p(x-y)}$ définit une distance ultramétrique sur $\mathbb{Q}$, v_p désignant la valuation p-adique sur $\mathbb{Q}$. Ainsi, tout comme $\mathbb{R}$ est la complétion de $\mathbb{Q}$ pour la distance usuelle, on peut prouver que $\mathbb{Q}_p$ est la complétion de $\mathbb{Q}$ pour cette distance, et que la structure de corps de $\mathbb{Q}_p$ est l'unique unique structure de corps topologique prolongeant celle de $\mathbb{Q}$.
Nous allons généraliser cette construction à des corps autres que $\mathbb{Q}$. Pour ce faire, introduisons une notion de distance compatible avec la structure de corps :

Définition 1.2.1. ***(Corps valués)***
On dit qu'un corps K est ***valué*** *s'il est muni d'une* ***valeur absolue****, c'est-à-dire d'une application $|.| : K \to \mathbb{R}^+$ telle que :*
(i) $\forall x \in K, |x| = 0 \Leftrightarrow x = 0$.
(ii) $\forall (x,y) \in K^2, |xy| = |x||y|$.
(iii) $\forall (x,y) \in K^2, |x+y| \leq |x| + |y|$.
Une valeur absolue sur K permet de définir une distance (et donc une topologie) sur K par $d(x,y) = |x-y|$. On dit que deux valeurs absolues sont ***équivalentes*** *lorsqu'elles induisent la même topologie sur K. Une* ***place*** *de K est une classe d'équivalence de valeurs absolues de K.*

Si K est un corps quelconque, pour chaque place $|.|$ de K, on peut construire le complété $K_{|.|}$ de K pour la topologie associée à $|.|$. Ce complété possède alors une unique structure de corps topologique prologeant celle de K et la valeur absolue de K se prolonge continûment en une valeur absolue de $K_{|.|}$.
En théorie des nombres, on s'intéresse beaucoup aux **corps de nombres**, c'est-à-dire aux extensions finies de $\mathbb{Q}$. Il convient donc de savoir quels corps on peut obtenir par complétion à partir d'un corps de nombres. Pour ce faire, il faut connaître les places d'un corps de nombres :

Théorème 1.2.2. ***(Théorème d'Ostrowski)***
Soit k un corps de nombres. Soit $\mathcal{O}_k$ l'ensemble des entiers algébriques contenus dans k. C'est un anneau appelé ***anneau des entiers*** *de k. Soit $\mathcal{P}$ l'ensemble des idéaux premiers non nuls de $\mathcal{O}_k$. Le groupe $Gal(\mathbb{C}/\mathbb{R})$ agit naturellement sur $Hom_{corps}(k,\mathbb{C})$. Soit R un ensemble de représentants de $Hom_{corps}(k,\mathbb{C})/Gal(\mathbb{C}/\mathbb{R})$. On a alors une bijection :*

$$\begin{aligned}
&\mathcal{P} \cup R \to \{places\ de\ k\} \\
&\mathfrak{p} \in \mathcal{P} \mapsto (|.|_{\mathfrak{p}} : x \mapsto e^{-v_{\mathfrak{p}}(x)}) \\
&\sigma \in R \mapsto (|.|_\sigma : x \mapsto |\sigma(x)|)
\end{aligned}$$

où $v_{\mathfrak{p}}(x)$ désigne le plus grand entier naturel v tel que $x \in \mathfrak{p}^v$. De plus, pour $\mathfrak{p} \in \mathcal{P}$, $k_{|.|_{\mathfrak{p}}}$ est ***un corps p-adique*** *(c'est-à-dire une extension finie de $\mathbb{Q}_p$) si $p \in \mathfrak{p}$, et pour $\sigma \in R$, $k_{|.|_\sigma}$ est isomorphe à $\mathbb{R}$ si $Im(\sigma) \subseteq \mathbb{R}$ et à $\mathbb{C}$ sinon.*

Remarque 1.2.3. La valeur absolue $|.|_{\mathfrak{p}}$ est équivalente à $|.|_{s,\mathfrak{p}} : x \mapsto s^{-v_{\mathfrak{p}}(x)}$ pour chaque réel $s > 1$. En général, on ne choisit pas $s = e$ comme dans le théorème précédent, mais plutôt le cardinal de $\mathcal{O}_k/\mathfrak{p}$.

Démonstration. On pourra aller voir la proposition 3.7 du chapitre II de [Neu99] pour le cas $k = \mathbb{Q}$. Il est assez facile d'en déduire le cas k quelconque. □

Remarque 1.2.4. Il sera utile dans la suite de savoir que, si k est un corps de nombres et v une place de k, alors $\mathrm{Gal}((k_v)^s/k_v)$ s'identifie à un sous-groupe de $\mathrm{Gal}(k^s/k)$, qui est défini à conjugaison près et que l'on appelle **sous-groupe de décomposition** en v.

Dans le cadre des corps de nombres, le principe de Hasse (qui est malheureusement faux en toute généralité) affirme que pour étudier une propriété sur un corps de nombres k, il faut et il suffit de l'étudier simultanément sur tous les complétés de k. Afin de tenir compte simultanément de tous les complétés de k, il est fort utile d'introduire les adèles et les idèles :

Définition 1.2.5. ***(Adèles et idèles)***
*Soit k un corps de nombres. Soit Ω l'ensemble des places de k. L'**anneau des adèles** de k est :*

$$A_k = \left\{ (x_v) \in \prod_{v \in \Omega} k_v / \text{pour presque toute place } v \text{ de } k,\ |x_v|_v \leq 1 \right\}$$

*où $|.|_v$ désigne le prolongement de v à k_v. Le **groupe des idèles** de k est $I_k = A_k^\times$. On remarque que $k^\times$ se plonge diagonalement dans I_k. Le groupe $C_k = I_k/k^\times$ est appelé **groupe des classes d'idèles**.*

Remarque 1.2.6. Dans la suite (partie 2.3 en particulier), nous aurons aussi besoin des groupes $I = \varinjlim_L I_L$ et $C = \varinjlim_L C_L$ où les limites inductives sont prises sur les extensions finies L de k.

2 Cohomologie galoisienne et théorème de Poitou-Tate

2.1 Généralités sur la cohomologie galoisienne

La cohomologie est un outil algébrique permettant de mesurer des obstructions à ce que certaines propriétés soient vraies. Ainsi, lorsque nous étudions certaines propriétés, nous pouvons faire apparaître naturellement certains groupes associés, appelés **groupes de cohomologie**, de sorte que :

- les groupes de cohomologie sont nuls dès que les propriétés étudiées sont vraies.
- intuitivement, plus les propriétés étudiées sont fausses, plus les groupes de cohomologie sont gros.

Par exemple, lorsque X est une variété différentielle, il est intéressant de se demander si toute k-forme différentielle fermée est exacte. Il est donc naturel d'introduire le quotient des k-formes différentielles fermées sur X par les k-formes différentielles exactes : ce quotient est le k-ième groupe de cohomologie de de Rham de X.
Donnons maintenant un exemple plus intéressant pour la suite. Pour chaque corps K, notons $\mathbb{P}^n(K)$ l'ensemble des droites vectorielles de K^{n+1}. C'est **l'espace projectif** de dimension n sur K et il joue un rôle fondamental en géométrie arithmétique. Il s'identifie au quotient de l'ensemble des vecteurs non nuls de K^{n+1} par la relation "deux vecteurs sont équivalents si, et seulement si, ils sont colinéaires". Fixons maintenant un corps K et soit K^s sa clôture séparable. Remarquons que $\mathbb{P}^n(K)$ s'injecte dans $\mathbb{P}^n(K^s)$ et que l'action évidente du groupe de Galois $G_K = \mathrm{Gal}(K^s/K)$ sur $(K^s)^{n+1}$ induit une action sur $\mathbb{P}^n(K^s)$. On voudrait alors montrer que $\mathbb{P}^n(K^s)^{G_K} = \mathbb{P}^n(K)$. L'inclusion $\mathbb{P}^n(K) \subseteq \mathbb{P}^n(K^s)^{G_K}$ est évidente. Soit maintenant $u \in (K^s)^{n+1}$ non nul tel que $K^s u \in \mathbb{P}^n(K^s)^{G_K}$. Cela entraîne que pour chaque $s \in G_K$, il existe $\phi(s) \in K^{s\times}$ tel que $s \cdot u = \phi(s)u$. Des calculs élémentaires prouvent que ϕ vérifie l'équation fonctionnelle $\phi(s_0 s_1) = \phi(s_0)s_0(\phi(s_1))$ et qu'il existe $\lambda \in K^{s\times}$ tel que $\lambda u \in K^{n+1}$ si, et seulement si, il existe $\mu \in K^{s\times}$ tel que $\phi(s) = s(\mu)\mu^{-1}$ pour tout $s \in G_K$. Par conséquent, $K^s u \in \mathbb{P}^n(K)$ si, et

seulement si, la classe de ϕ dans

$$H^1(G_K, K^{s\times}) := \frac{\{f : G_K \to K^{s\times} / \forall (s_0, s_1) \in G_K^2, f(s_0 s_1) = f(s_0) s_0(f(s_1))\}}{\{G_K \to K^{s\times}, s \mapsto s(\mu)\mu^{-1} / \mu \in K^{s\times}\}}$$

est nulle. Il est en fait possible de montrer que cela est toujours le cas (voir 2.1.4(ii)), ce qui établit l'égalité $\mathbb{P}^n(K^s)^{G_K} = \mathbb{P}^n(K)$.
Ainsi, en s'inspirant de l'exemple précédent, il est naturel d'introduire le groupe :

$$H^1(G, M) = \frac{\{f : G \to M / \forall (s_0, s_1) \in G^2, f(s_0 s_1) = f(s_0) + s_0 \cdot f(s_1)\}}{\{G \to M, s \mapsto s \cdot m - m / m \in M\}}$$

où G désigne un groupe et M un groupe abélien muni d'une action à gauche de G vérifiant $s \cdot (m_1 + m_2) = s \cdot m_1 + s \cdot m_2$ pour $s \in G$ et $m_1, m_2 \in M$. Plus généralement, on définit :

Définition 2.1.1. ***(Cohomologie des groupes abstraits)***
Soit G un groupe.
*(i) Un **G-module** est un groupe abélien M muni d'une action à gauche de G vérifiant $s \cdot (m_1 + m_2) = s \cdot m_1 + s \cdot m_2$ pour $s \in G$ et $m_1, m_2 \in M$.*
(ii) Soit M un G-module. Considérons la suite :

$$\mathcal{F}(G^0, M) \xrightarrow{d^0} \mathcal{F}(G^1, M) \xrightarrow{d^1} \mathcal{F}(G^2, M) \xrightarrow{d^2} \dots$$

où $G^0 = \{1\}$ par convention, $\mathcal{F}(G^i, M)$ désigne l'ensemble des fonctions de G^i vers M et

$$d^i f(s_0, ..., s_i) = s_0 f(s_1, ..., s_i) + \sum_{k=1}^{i} (-1)^k f(s_0, ..., s_{k-1}s_k, ..., s_i) + (-1)^{i+1} f(s_0, ..., s_{i-1})$$

pour $f \in \mathcal{F}(G^i, M)$. Cette suite est un complexe au sens où $d^{i+1} \circ d^i = 0$. Par conséquent, $Im(d^i) \subseteq Ker(d^{i+1})$ et on appelle r-ième groupe de cohomologie de M le groupe $H^r(G, M) = Ker(d^r)/Im(d^{r-1})$.

Pour ceux qui connaissent le formalisme des foncteurs dérivés, on peut montrer que, si G est un groupe, le foncteur $H^r(G, -)$ est en fait le r-ième foncteur dérivé à droite du foncteur exact à gauche $M \to M^G$ allant de la catégorie des G-modules vers la catégorie des groupes abéliens.
En géométrie arithmétique, nous voulons utiliser les constructions précédentes en prenant pour G le groupe de Galois d'une extension algébrique galoisienne (éventuellement infinie), disons $G = \mathrm{Gal}(K/k)$. Dans ce cas, on sait que G est la limite projective des groupes finis $\mathrm{Gal}(L/k)$ où L décrit les extensions finies galoisiennes de k contenues dans K. Un tel groupe, limite projective de groupes finis, est dit **profini** et est muni d'une topologie naturelle, chaque groupe fini apparaissant dans la limite projective étant muni de la topologie discrète. Or la construction précédente des groupes de cohomologie ne tient pas compte des aspects topologiques. Il convient donc de la modifier légèrement :

Définition 2.1.2. ***(Cohomologie des groupes profinis)***
Soit G un groupe profini.

*(i) Un **G-module discret** est un G-module M muni de la topologie discrète tel que l'application $G \times M \to M, (g, m) \mapsto gm$ est continue.*

*(ii) Soit M un G-module discret. Le **r-ième groupe de cohomologie** $H^r(G, M)$ de M est alors défini exactement comme dans la définition 2.1.1(ii) en remplaçant $\mathcal{F}(G^i, M)$ par l'espace des fonctions continues de G^i vers M. C'est encore le r-ième foncteur dérivé à droite du foncteur exact à gauche $M \mapsto M^G$ allant de la catégorie des G-modules discrets vers celle des groupes*

abéliens. Cela impose en particulier que, pour chaque suite exacte $0 \to M_1 \to M_2 \to M_3 \to 0$ *de* G*-modules discrets, on dispose d'une suite exacte longue*

$$... \to H^{r-1}(G, M_3) \to H^r(G, M_1) \to H^r(G, M_2) \to H^r(G, M_3) \to H^{r+1}(G, M_1) \to ...$$

Remarque 2.1.3. Si G est un groupe profini, H est un sous-groupe fermé et M un G-module discret, on voit immédiatement que l'on peut définir naturellement un morphisme dit **de restriction** $H^r(G, M) \to H^r(H, M)$. De même, si H est en plus distingué, on peut définir un morphisme dit **d'inflation** $H^r(G/H, M^H) \to H^r(G, M)$.

Dans la suite, lorsque G est un groupe profini et M un G-module discret, $H^r(G, M)$ désignera toujours le groupe défini dans 2.1.2(ii) et non dans 2.1.1(ii). Il se trouve que la cohomologie des groupes profinis se ramène aisément à la cohomologie des groupes finis. En effet, les morphismes d'inflation induisent un isomorphisme naturel $\varinjlim_U H^r(G/U, M^U) \to H^r(G, M)$, où U décrit les sous-groupes ouverts distingués de G et les flèches de transition sont les morphismes d'inflation, et G étant profini, les quotients G/U sont finis. En particulier, si $G = \mathrm{Gal}(K/k)$ pour K/k une extension algébrique galoisienne, on a $H^r(G, M) = \varinjlim_L H^r(\mathrm{Gal}(L/k), M^{\mathrm{Gal}(K/L)})$, la limite inductive étant prise sur les extensions finies galoisiennes L de k contenues dans K. Dans la suite, on notera plutôt $H^r(G, M) = H^r(K/k, M)$ et $H^r(k^s/k, M) = H^r(k, M)$, où k^s désigne la clôture séparable de k.
Soit maintenant k un corps quelconque, et rappelons que G_k désigne son groupe de Galois absolu. Deux exemples fondamentaux de G_k-modules discrets sont k^s et $k^{s,\times}$ et il est donc intéressant d'étudier leur cohomologie :

Proposition 2.1.4. *(i)* ***(Cohomologie de*** $\mathbb{G}_a$***)*** *Pour tout* $r > 0$, $H^r(k, k^s) = 0$.
(ii) ***(Théorème de Hilbert 90)*** *On a* $H^1(k, k^{s,\times}) = 0$.

Démonstration.

(i) * Soit $r > 0$. On sait que $H^r(k, k^s) = \varinjlim_L H^r(L/k, L)$, où L décrit les extensions finies galoisiennes de k contenues dans k^s. Or, d'après le théorème de la base normale, $\mathrm{Hom}_{\mathrm{Gal}(L/k)}(M, L) \cong \mathrm{Hom}_{\mathbb{Z}}(M, k)$, et donc $H^r(L/k, L) = \mathrm{Ext}^r_{\mathrm{Gal}(L/k)}(\mathbb{Z}, L) \cong \mathrm{Ext}^r_{\{1\}}(\mathbb{Z}, k) = 0$. Cela impose que $H^r(k, k^s) = 0$.

(ii) On sait que $H^1(k, k^{s,\times}) = \varinjlim_L H^1(L/k, L^\times)$, où L décrit les extensions finies galoisiennes de k contenues dans k^s. Soit $f : \mathrm{Gal}(L/k) \to L^\times$ non nulle telle que $f(s_0 s_1) = f(s_0) s_0(f(s_1))$. Comme les éléments de $\mathrm{Gal}(L/k)$ sont linéairement indépendants, il existe $c \in L^\times$ tel que $b = \sum_{s \in \mathrm{Gal}(L/k)} f(s) s(c)$ est non nul. On vérifie alors aisément que $f(s) = b/s(b)$ pour tout $s \in \mathrm{Gal}(L/k)$. Par conséquent $H^1(L/k, L^\times) = 0$ et $H^1(k, k^{s,\times}) = 0$. □

On en déduit que la cohomologie du G_k-module k^s n'est pas intéressante. Par contre, la cohomologie de $k^{s,\times}$ est beaucoup plus compliquée, puisqu'elle n'est pas forcément nulle à partir du rang 2. En particulier, le groupe $\mathrm{Br}(k) = H^2(k, k^{s,\times})$, appelé **groupe de Brauer de** k, est un invariant important associé au corps k.

2.2 Cohomologie des corps p-adiques

Considérons K un corps p-adique. Notons $\mathcal{O}_K$ son anneau des entiers (c'est-a-dire l'ensemble des éléments de K de valeur absolue inférieure ou égale à 1) et k son corps résiduel (c'est-à-dire le quotient de $\mathcal{O}_K$ par son unique idéal maximal, qui est constitué des éléments de valeur absolue strictement plus petite que 1). La première étape pour comprendre la cohomologie des corps p-adiques consiste à calculer le groupe de Brauer :

Théorème 2.2.1. ***(Groupe de Brauer d'un corps p-adique)***
On a un isomorphisme $inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z}$ appelé ***invariant local****.*

Démonstration. * Notons K^{nr} l'extension maximale non ramifiée de K et $\mathcal{O}_K^{nr}$ son anneau des entiers. D'après le théorème 1 du chapitre XII de [Ser68] et son corollaire, $\mathrm{Br}(K) = H^2(K^{nr}/K, K^{nr,\times})$. À l'aide du lemme 2 du même chapitre et en passant à la limite, on prouve que $H^r(K^{nr}/K, \mathcal{O}_K^{nr,\times}) = 0$. Par conséquent, comme on dispose d'un isomorphisme de $\mathrm{Gal}(K^{nr}/K)$-modules $K^{nr,\times} \cong \mathcal{O}_K^{nr,\times} \oplus \mathbb{Z}$, on a $\mathrm{Br}(K) \cong H^2(K^{nr}/K, \mathbb{Z}) \cong H^1(K^{nr}/K, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_c(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$. Pour plus de détails, voir le chapitre XII de [Ser68]. □

Notons μ_m l'ensemble des racines m-ièmes de l'unité dans K^s. Puisqu'on dispose d'une suite exacte $1 \to \mu_m \to K^{s,\times} \to K^{s,\times} \to 1$, le théorème de Hilbert 90 et le théorème précédent imposent que $H^1(K, \mu_m) \cong K^\times/K^{\times^m}$ et $H^2(K, \mu_m) \cong \mathbb{Z}/m\mathbb{Z}$, qui sont finis. Plus généralement, on dispose du théorème de finitude suivant :

Théorème 2.2.2. ***(Théorèmes d'annulation et de finitude)***
(i) Pour $r > 2$ et M un G_K-module de torsion, $H^r(K, M) = 0$.
(ii) Pour $r \geq 0$ et M un G_K-module fini, $H^r(K, M)$ est fini.

Démonstration. *
(i) On écrit la suite spectrale de Hochschild-Serre $H^r(k^s/k, H^s(K^{nr}, M)) \Rightarrow H^{r+s}(K, M)$. Or d'après les résultats de dimension cohomologique de la section VI.5 de [NSW08], $H^r(k^s/k, H^s(K^{nr}, M))$ est nul dès que $r + s > 2$. On en déduit que $H^r(K, M)$ est nul dès que $r > 2$.
(ii) Comme M est fini, on trouve une extension finie galoisienne L telle que l'action de G_L sur M est triviale. Du coup, on a un isomorphisme de G_L-modules $M \cong \bigoplus_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$ pour certains entiers n_i. Quitte à augmenter L, on peut supposer que les racines n_i-ièmes de l'unité sont dans L, pour chaque i, ce qui permet d'écrire $M \cong \bigoplus_i \mu_{n_i}$. Par conséquent, à l'aide de (i) et des remarques précédant ce théorème, $H^r(L, M)$ est fini pour tout r. La suite spectrale $H^r(L/K, H^s(L, M)) \Rightarrow H^{r+s}(K, M)$ permet alors de conclure.

□

Pour terminer, nous allons énoncer un théorème de dualité fondamental, dû à John Tate :

Théorème 2.2.3. ***(Théorème de dualité de Tate)***
Soit M un G_K-module fini et notons $M^D = Hom_{\mathbb{Z}}(M, K^{s,\times})$. Pour chaque $r \in \mathbb{Z}$, il existe un accouplement parfait de groupes abéliens de torsiob $H^r(K, M) \times H^{2-r}(K, M^D) \to Br(K) \cong \mathbb{Q}/\mathbb{Z}$.

Remarque 2.2.4. Si A et B sont des groupes abéliens, on dit qu'un application bilineaire $A \times B \to \mathbb{Q}/\mathbb{Z}$ est un accouplement parfait si elle induit des isomorphismes $A \cong \mathrm{Hom}(B, \mathbb{Q}/\mathbb{Z})$ et $B \cong \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$.

Démonstration. * La preuve de ce théorème est assez délicate. Il faut d'abord établir que $(G_K, K^{s\times})$ est une formation de classes grâce au théorème de Hilbert 90 et à l'invariant local. L'application du théorème de dualité pour les formations de classes (théorème 1.8 de la partie I de [Mil06]) permet alors de conclure. Le lecteur intéressé pourra aller voir le corollaire 2.3 du chapitre I de [Mil06]. □

2.3 Cohomologie des corps de nombres

Soit k un corps de nombres. Dans cette section, nous allons étudier la cohomologie des corps de nombres comme nous l'avons fait pour les corps p-adiques et nous allons voir que la situation est nettement plus compliquée. Pour ce faire, le point de départ est la **théorie du corps de**

classes, et en particulier l'**axiome du corps de classes**, qui permet d'établir un résultat qui joue le même rôle que le théorème de Hilbert 90 dans le cadre des corps p-adiques :

Théorème 2.3.1. ***(Axiome du corps de classes)***
(i) Soit K une extension cyclique de k. Alors $H^1(K/k, C_K) = 0$.
(ii) Rappelons que $C = \varinjlim_L C_L$ où la limite inductive est prise sur les extensions finies L de k. On a $H^1(k, C) = 0$.

Démonstration. *

(i) Le lecteur pourra aller voir le théorème 4.4 du chapitre VI de [Neu99].

(ii) À l'aide de (i) et de résultats élémentaires de cohomologie galoisienne, on montre successivement que l'égalité $H^1(L/k, C_L) = 0$ est vraie :
- lorsque $\mathrm{Gal}(L/k)$ est un p-groupe.
- quelle que soit l'extension galoisienne finie L/k.

Un passage à la limite prouve alors que $H^1(k, C) = 0$. On pourra aller voir le corollaire 8.1.13 de [NSW08]. □

Le deuxième résultat de la théorie du corps de classes dont nous avons besoin est la **suite de Brauer-Hasse-Noether**, qui relie le groupe de Brauer d'un corps de nombres aux groupes de Brauer de ses complétés et qui permet d'établir un isomorphisme jouant le rôle de l'invariant local :

Théorème 2.3.2. ***(Suite de Brauer-Hasse-Noether)***
(i) La suite $0 \to Br(k) \to \bigoplus_v Br(k_v) \to \mathbb{Q}/\mathbb{Z} \to 0$, où v décrit toutes les places de k et où la flèche $\bigoplus_v Br(k_v) \to \mathbb{Q}/\mathbb{Z}$ est $\sum_v inv_{k_v}$, est exacte.
(ii) On a un isomorphisme $inv_k : H^2(k, C) \to \mathbb{Q}/\mathbb{Z}$.

Démonstration. *
(i) Le lecteur pourra aller voir le théorème 8.1.17 de [NSW08].
(ii) On prouve que la suite $0 \to \mathrm{Br}(k) \to H^2(k, I) \to H^2(k, C) \to 0$ est exacte (voir la proposition 8.1.20 de [NSW08]). Or, comme $H^2(k, -)$ commute avec les limites inductives, $H^2(k, I) = \bigoplus_v \mathrm{Br}(k_v)$. En comparant cette suite exacte à celle de Brauer-Hasse-Noether, on obtient un isomorphisme $H^2(k, C) \to \mathbb{Q}/\mathbb{Z}$.

□

Les deux théorèmes précédents permettent alors d'établir un théorème analogue au théorème de dualité de Tate, cette fois-ci pour les corps de nombres :

Théorème 2.3.3. ***(Théorème de dualité)***
Soit M un G_k-module discret de type fini. Pour chaque $r \geq 1$, on a un accouplement parfait de groupes finis : $Ext^r_{G_k}(M, C) \times H^{2-r}(G_k, M) \to \mathbb{Q}/\mathbb{Z}$.

Remarque 2.3.4. Ici les $\mathrm{Ext}^r_{G_k}(M, -)$ sont les foncteurs dérivés du foncteur qui à un G_k-module discret N associe le groupe abélien des morphismes de G_k-modules discrets de M dans N. Pour ceux qui ne savent pas ce que cela veut dire, il convient simplement de comprendre que le théorème précédent est l'analogue du théorème de dualité de Tate pour les corps de nombres.

Démonstration. * Les théorèmes 2.3.1 et 2.3.2 permettent d'établir que (G_k, C) est une formation de classes. Comme pour le théorème de dualité de Tate, l'application du théorème de dualité pour les formations de classes permet alors de conclure. On pourra aller voir le théorème 4.6 de la partie I de [Mil06]. □

2.4 Relier la cohomologie des corps de nombres à la cohomologie des corps p-adiques : le théorème de Poitou-Tate

Attention : À partir de maintenant, lorsque $K = \mathbb{R}$, on note $H^0(K,M) = M^{\mathbb{R}}/\{cm - m/m \in M\}$ où c désigne la conjugaison complexe, et lorsque $K = \mathbb{C}$, on note $H^0(K,M) = 0$. Ce sont les **groupes de cohomologie modifiée de Tate**. Nous faisons cette précision pour que les théorèmes qui suivent soient vrais, mais il ne faut pas lui accorder trop d'importance, puisque ce n'est qu'un détail technique.

Fixons un corps de nombres k et notons Ω l'ensemble des places de k. Nous sommes maintenant en mesure de présenter le théorème de Poitou-Tate, qui permet de relier la cohomologie des corps de nombres à celle des corps p-adiques. Pour ce faire, pour chaque G_k-module discret M, il convient de définir les **groupes de Tate-Shafarevich** pour $r = 1, 2$:

$$Ш^r(k,M) = \mathrm{Ker}\left(\beta^r : H^r(k,M) \to \prod_{v\in\Omega} H^r(k_v,M)\right)$$

où β^r est induit par les restrictions. Le théorème de Poitou-Tate exprime alors le lien entre $H^r(k,M)$ et $\prod_{v\in\Omega} H^r(k_v,M)$:

Théorème 2.4.1. ***(Théorème de Poitou-Tate)***
Soit M un G_k-module discret fini. Alors :
(i) Pour $r \geq 3$, on a $H^r(G_k,M) \cong \bigoplus_{v\in\Omega_{\mathbb{R}}} H^r(k_v,M)$, où $\Omega_{\mathbb{R}}$ désigne les places $v \in \Omega$ telles que $k_v = \mathbb{R}$.
(ii) L'image de β^2 est contenue dans $\bigoplus_{v\in\Omega} H^2(k_v,M)$ et il est possible de définir un sous-groupe $\mathbb{P}^1(k,M)$ de $\prod_{v\in\Omega} H^1(k_v,M)$ contenant l'image de β^1 et s'insérant dans une suite exacte à 9 termes :

$$\begin{tikzcd}
0 \arrow[r] & H^0(k,M) \arrow[r, "\beta^0"] & \prod_{v\in\Omega} H^0(k_v,M) \arrow[r] & H^2(k,M^D)^* \arrow[d] \\
& H^1(k,M^D)^* \arrow[d] & \mathbb{P}^1(k,M) \arrow[l] & H^1(k,M) \arrow[l, "\beta^1"'] \\
& H^2(k,M) \arrow[r, "\beta^2"] & \bigoplus_{v\in\Omega} H^2(k_v,M) \arrow[r] & H^0(k,M^D)^* \arrow[r] & 0
\end{tikzcd}$$

où $M^D = Hom_{\mathbb{Z}}(M, k^{s,\times})$ est le dual de Cartier de M et $H^* = Hom(H, \mathbb{Q}/\mathbb{Z})$ désigne le dual de Pontryagin du groupe abélien de torsion H.
(iii) Il existe une dualité parfaite de groupes finis :

$$Ш^1(k,M^D) \times Ш^2(k,M) \to \mathbb{Q}/\mathbb{Z}.$$

Remarque 2.4.2. Le théorème de Poitou-Tate a été énoncé pour la première fois par John Tate en 1962 lors du Congrès International de Mathématiques ([Tat63]). Il a été prouvé de manière indépendante par Tate dans une lettre à Springer en 1966 et par Poitou dans [Poi67] en 1967 dans un cas plus général.

Démonstration. * On écrit la suite exacte $0 \to k^{s,\times} \to I \to C \to 0$ puis on applique le foncteur $\mathrm{Hom}_{G_k}(M^D, -)$. Il faut alors calculer les Ext qui apparaissent :
- on prouve par des techniques élémentaires (suite spectrale des Ext) que $\mathrm{Ext}^r_{G_k}(M^D, k^s) = H^r(k,M)$.

- par des calculs fins d'approximation à l'aide de limites inductives, on prouve que $\mathrm{Ext}^r_{G_k}(M^D, I)$ est $\prod_{v\in\Omega} H^0(k_v, M)$ si $r = 0$, $\bigoplus_{v\in\Omega} H^2(k_v, M)$ si $r = 2$, $\bigoplus_{v\in\Omega_\mathbb{R}} H^r(k_v, M)$ si $r > 2$, et on calcule $\mathrm{Ext}^1_{G_k}(M^D, I) = \mathbb{P}^1(k, M)$.
- grâce au théorème de dualité 2.3.3, on a $\mathrm{Ext}^r_{G_k}(M^D, C) = H^{2-r}(G_k, M^D)^*$.

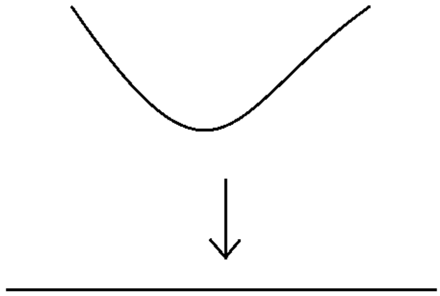
Cela permet d'obtenir (i) et (ii). Quant à (iii), il découle de (ii) et du théorème de dualité de Tate. Pour plus de détails, on pourra aller voir le théorème 4.10 de la partie I de [Mil06]. □

3 Approche du théorème de Poitou-Tate par la cohomologie étale

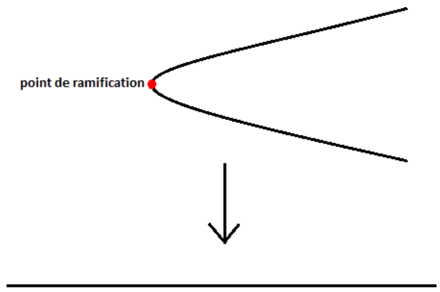
3.1 Généralités sur la cohomologie étale

Nous allons faire le point sur certaines notions de géométrie algébrique. À chaque espace topologique X on peut associer la catégorie `Ouv` de ses ouverts, dont les morphismes sont les inclusions. Un **préfaisceau** sur X est alors un foncteur contravariant de `Ouv` vers la catégorie des groupes abéliens. Un **faisceau** est un préfaisceau vérifiant certaines propriétés de recollement qui moralement signifient que si les U_i sont des ouverts de X et si on se donne pour chaque i une fonction f_i sur U_i de sorte que f_i et f_j coïncident sur $U_i \cap U_j$, alors il existe une unique fonction sur $\bigcup_i U_i$ prolongeant les f_i. Si F est un faisceau sur X et x un élément de X, alors on appelle **tige de F en x** le groupe $\varinjlim_U F(U)$ où U décrit les ouverts de X contenant x. Cette notion joue un rôle fondamental puisque de nombreuses propriétés des faisceaux peuvent être lues dans les tiges.
Pour généraliser ces constructions, Grothendieck a adopté un autre point de vue, en observant que la catégorie `Ouv` est équivalente à la catégorie des inclusions $U \to X$ d'un ouvert U de X dans X. Plus généralement, on peut, si l'on veut, remplacer ces catégories par d'autres catégories de fonctions $Y \to X$ vérifiant certaines conditions et munies d'une notion de recouvrement : par exemple, on peut considérer la catégorie $\mathcal{C}$ des fonctions continues $Y \to X$ et dire qu'une famille $\{f_i : Y_i \to Y\}$ de morphismes de $\mathcal{C}$ (applications continues compatibles avec les applications $Y_i \to X$ et $Y \to X$) est un recouvrement lorsque $\bigcup_i f_i(Y_i) = Y$. La donnée d'une telle catégorie et d'une famille de recouvrements est appelée **topologie de Grothendieck**. Cette construction généralise la notion d'espace topologique.
Dans le cadre de la géométrie arithmétique, il est particulièrement intéressant de se pencher sur le cas où X est un schéma (un espace topologique muni d'une structure supplémentaire et qui localement est isomorphe au spectre d'un anneau) muni de la topologie de Grothendieck suivante :

- Catégorie : morphismes étales $Y \to X$. En particulier, ce sont des morphismes sans points de ramification. Par exemple :



Morphisme étale



Morphisme non étale

Pour la définition précise de morphisme étale, on pourra se référer à la partie 2.3 de [Fu11] ou à la partie I.3 de [Mil80].

• Recouvrements : familles de morphismes étales $\{f_i : Y_i \to Y\}$ telles que $\bigcup_i f_i(Y_i) = Y$.

Cette topologie est appelée **site étale** de X. Sur le site étale de X, il est possible définir comme dans le cadre des espaces topologiques usuels des notions de préfaisceau, de faisceau et de tige d'un faisceau en un point de X.

Exemple 3.1.1. (i) Le foncteur $\mathrm{Hom}(-, \mathrm{Spec}\, \mathbb{Z}[T, T^{-1}])$ est un faisceau sur X, appelé **groupe multiplicatif** et noté $\mathbb{G}_m$. De même, si A est un groupe abélien, le foncteur $\mathrm{Hom}_X(-, \coprod_A X)$ est un faisceau sur X, que l'on note toujours A. Un tel faisceau est dit **constant**.

(ii) Si F et G sont deux faisceaux sur X, alors on peut définir un nouveau faisceau sur X, noté $\underline{\mathrm{Hom}}_X(F, G)$ par $Y \mapsto \mathrm{Hom}_Y(F|_Y, G|_Y)$ où $F|_Y$ et $G|_Y$ sont les restrictions de F et G à Y.

Considérons maintenant le foncteur exact à gauche qui à un faisceau F sur X associe le groupe abélien $F(X)$ (appelé **groupe des sections globales**) et notons $H^r(X, -)$ son r-ième foncteur dérivé : c'est la **cohomologie étale** des faisceaux sur X. Pour ceux qui ne savent pas ce que cela signifie, il suffit de comprendre que, comme dans la section 2, les foncteurs $H^r(U, -)$ mesurent certains défauts (en particulier la non exactitude du foncteur des sections globales). Sous de bonnes hypothèses, il est possible de donner une description explicite de $H^r(X, -)$: le lecteur intéressé pourra aller voir le corollaire 2.5 et le théorème 2.17 de [Mil80].

Remarque 3.1.2. Comme dans toute théorie cohomologique, à chaque suite exacte courte de faisceaux $0 \to F_1 \to F_2 \to F_3 \to 0$ est associée un suite exacte longue $\ldots \to H^r(X, F_1) \to H^r(X, F_2) \to H^r(X, F_3) \to \ldots$.

L'étude de la cohomologie étale est particulièrement intéressant parce qu'elle généralise la cohomologie galoisienne. En effet, si X est le spectre d'un corps k et F est un faisceau sur X de tige M, alors M est un $\mathrm{Gal}(k^s/k)$-module discret et $H^r(X, F) = H^r(k, M)$. La cohomologie étale coïncide donc avec la cohomologie galoisienne lorsque la géométrie de X est triviale, c'est-à-dire dans le cas purement arithmétique. Plus généralement, lorsque le schéma X est le spectre d'un anneau intègre A de corps des fractions k et F un faisceau X, la tige M au point (0) (point générique) de F est un G_k-module discret et on dispose d'un morphisme de "restriction" reliant la cohomologie étale à la cohomologie galoisienne : $H^r(U, F) \to H^r(k, M)$. Ainsi, lorsque X est un schéma quelconque, la cohomologie étale permet de tenir compte simultanément des propriétés arithmétiques, encodées dans la cohomologie des tiges, et des propriétés géométriques, encodées dans la cohomologie sur les ouverts de X.

Pour terminer, remarquons que, lorsque X est le spectre de l'anneau des entiers d'un corps de nombres k, le théorème d'Ostrowski impose que chaque point de X différent de (0) (point générique) correspond à une place de k. Dans ce contexte, nous aurons besoin de la cohomologie à support compact, que nous n'allons pas définir proprement ici. Pour comprendre la suite, il suffira de savoir que, pour U un ouvert de X, il est possible de définir des foncteurs $H_c^r(U, -)$ allant des faisceaux sur U vers les groupes abéliens, qui transforment une suite exacte courte de faisceaux sur U en une suite exacte longue (voir remarque précédente pour comprendre ce que cela signifie), et qui sont reliés à la cohomologie étale par une suite exacte :

$$... \to H_c^r(U, F) \to H^r(U, F) \to \bigoplus_{v \notin U} H^r(k_v, M) \to ...$$

où M désigne la tige de F au point (0) et la somme directe est prise sur toutes les places de k qui ne sont pas dans U (même celles qui sont paramétrées par les morphismes de corps de k dans $\mathbb{C}$). Pour plus de détails sur la cohomologie étale, on renvoie le lecteur au livre [Tam94], et pour la cohomologie à support compact, au paragraphe 2 de la partie II de [Mil06].

3.2 Le théorème d'Artin-Verdier

Donnons-nous un corps de nombres k et notons X le spectre de son anneau des entiers. La preuve du théorème de Poitou-Tate que nous allons présenter dans la suite est fondée sur le théorème de dualité assez difficile suivant :

Théorème 3.2.1. ***(Théorème d'Artin-Verdier)***
Soit U un ouvert non vide de X. Soit F un faisceau localement constant sur U à tiges finies tel qu'il existe un entier m qui n'est contenu dans aucun élément de U et qui vérifie $mF = 0$. Notons $F^D = \underline{Hom}_U(F, \mathbb{G}_m)$. Il existe alors un accouplement parfait de groupes finis :

$$H^r(U, F^D) \times H_c^{3-r}(U, F) \to \mathbb{Q}/\mathbb{Z}.$$

Démonstration. * Comme les foncteurs $H_c^r(U, -)$ transforment des suites exactes courtes en des suites exactes longues, on dispose d'un accouplement :

$$\mathrm{Ext}_U^r(F, \mathbb{G}_m) \times H_c^{3-r}(U, F) \to H_c^3(U, \mathbb{G}_m).$$

Il est possible de montrer que $H_c^3(U, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$, ce qui fournit un morphisme $\alpha^r(U, F)$: $\mathrm{Ext}_U^r(F, \mathbb{G}_m) \to (H_c^{3-r}(U, F))^*$. Les étapes à suivre sont alors les suivantes :
1. Montrer que $\alpha^r(U, F)$ est un isomorphisme si F est à support fini.
2. Utiliser 1. pour montrer que $\alpha^r(U, F)$ est un isomorphisme pour tout r si, et seulement si, $\alpha^r(V, F)$ l'est pour un certain ouvert V de U.
3. Montrer que $H_c^r(U, F)$ est nul pour r assez grand ($r \geq 4$) : pour ce faire, il faut comparer la cohomologie étale à la cohomologie galoisienne.
4. Montrer que $\mathrm{Ext}_U^r(F, \mathbb{G}_m)$ est nul pour r assez grand ($r \geq 4$) lorsque K n'a pas de places réelles.
5. Étudier le comportement de α^r vis-à-vis de la normalisation : montrer que $\alpha^r(U_n, F_n)$ est un isomorphisme si, et seulement si, $\alpha^r(U, \pi_* F_n)$ l'est, où $\pi : U_n \to U$ désigne la normalisation de U dans une extension finie L de k et F_n un faisceau localement constant à tiges finies sur U_n.
6. Se ramener au cas où k n'a pas de places réelles et $U = X$. Pour ce faire, montrer par récurrence sur r que, si $\alpha^r(X, F)$ est un isomorphisme pour tout r lorsque k est un corps de nombres sans places réelles et F un faisceau localement constant à tiges finies sur X, alors $\alpha^r(U, F)$ est un isomorphisme quel que soit le corps de nombres k, l'ouvert U de X et le faisceau localement constant à tiges finies F sur U : l'initialisation découle de l'étape 3., et on

passe à la récurrence en exploitant une suite exacte de la forme $0 \to F_1 \to F \to \pi_*\pi^*F \to 0$, où π est la normalisation de U dans une extension finie galoisienne de k sans places réelles, et en utilisant l'étape 5. pour étudier $\pi_*\pi^*F$ et l'étape 2. pour passer de U à X.

7. Montrer que le faisceau F s'injecte dans un faisceau de la forme $\pi_*F_n \oplus F_f$ où $\pi : U_n \to U$ est la normalisation de U dans une extension finie L de k sans places réelles, F_n un faisceau constant sur U_n et F_f est à support fini.
8. Montrer que, sous de bonne hypothèses, si $\alpha^r(X,F)$ est un isomorphisme quel que soit le corps k sans places réelles, le faisceau localement constant à tiges finies F et $r > r_0$, alors $\alpha^{r_0}(X,F)$ est un isomorphisme quel que soit le corps k sans places réelles et le faisceau localement constant à tiges finies F : pour ce faire, on utilise l'étape 7. pour avoir une injection $F \hookrightarrow \pi_*F_n \oplus F_f$, puis les étapes 5. et 1. permettent d'étudier π_*F_n et F_f respectivement.
9. Montrer que, pour tout corps de nombres k sans places réelles, tout faisceau localement constant à tiges finies F sur X et tout r, $\alpha^r(X,F)$ est un isomorphisme : l'étape 4. donne le cas $r > 3$, puis l'étape 8. permet de déduire successivement les cas $r = 3, r = 2, r = 1, r = 0$, et finalement l'étape 3. établit le cas $r < 0$.
10. Les étapes 6. et 9. montrent que $\alpha^r(U,F)$ est toujours un isomorphisme.
11. Montrer que $H^r(U,F^D) \cong \mathrm{Ext}^r_U(F,\mathbb{G}_m)$.

Pour plus de détails, on renvoie au paragraphe 3 de la partie II de [Mil06] ou à la section 2 de [Izq13]. □

3.3 Le théorème de Poitou-Tate à partir du théorème d'Artin-Verdier

En reprenant les notations des sections 2.4 et 3.2, nous allons maintenant donner les étapes principales d'une preuve du théorème de Poitou-Tate utilisant le théorème d'Artin-Verdier. Cette preuve, fortement inspirée de l'article de David Harari et Tamas Szamuely [HS13] qui démontre un théorème de Poitou-Tate pour les corps de fonctions sur des corps p-adiques, a fait l'objet d'un mémoire que j'ai réalisé sous la direction de David Harari ([Izq13]) :

1. Passage de la cohomologie galoisienne à la cohomologie étale : montrer qu'il existe un faisceau F localement constant sur un ouvert de X dont la tige au point générique est M. On remarque que la tige de F^D au point générique est M^D. Pour simplifier, dans la suite, on supposera que F est un faisceau localement constant sur X tout entier.
2. Interprétation du deuxième groupe de Tate-Shafarevich dans le cadre de la cohomologie étale : pour U ouvert de X, noter $\mathcal{D}^2(U,F^D)$ l'image de la composée $H^2_c(U,F^D) \to H^2(U,F^D) \to H^2(k,M^D)$ (rappelons que M^D est la tige au point générique de F^D), et montrer que $\mathcal{D}^2(U,F^D) = Ш^2(k,M^D)$.
3. Interprétation du premier groupe de Tate-Shafarevich dans le cadre de la cohomologie étale : pour U ouvert de X, noter $D^1_{sh}(U,F)$ le noyau de $H^1(U,F) \to \prod_v H^1(k_v,M)$ (v décrivant les places de k), et montrer que $Ш^1(k,M) = \varinjlim_U D^1_{sh}(U,F)$.
4. Construire des suites exactes qui font intervenir $\mathcal{D}^2(U,F^D)$ et $D^1_{sh}(U,F)$: montrer qu'on a des suites exactes $\bigoplus_v H^1(k_v,M^D) \to H^2_c(U,F^D) \to \mathcal{D}^2(U,F^D) \to 0$ et $0 \to D^1_{sh}(U,F) \to H^1(U,F) \to \prod_v H^1(k_v,M)$.
5. Montrer que $\mathcal{D}^2(U,F^D)$ et $D^1_{sh}(U,F)$ sont duaux l'un de l'autre : remarquer, grâce au théorème de dualité de Tate et au théorème d'Artin-Verdier, que $(\prod_v H^1(k_v,M))^* \cong \bigoplus_v H^1(k_v,M^D)$ et que $(H^1(U,F))^* \cong H^2_c(U,F^D)$. Déduire que les suites de 4. sont duales l'une de l'autre, et donc que $D^1_{sh}(U,F)^* \cong \mathcal{D}^2(U,F^D)$.
6. Conclure : En passant à la limite dans l'isomorphisme de l'étape 5. et en utilisant 2. et 3., on obtient un isomorphisme $Ш^1(k,M)^* \cong Ш^2(k,M^D)$.

Pour plus de détails, on renvoie à la section 3 de [Izq13].

3.4 Quelques remarques

La preuve que nous venons de donner du théorème de Poitou-Tate nécessite plus de connaissances que la démontration classique (résumée dans la section 2.4), puisqu'elle fait appel à la cohomologie étale, à la cohomologie à support compact et au théorème d'Artin-Verdier. Cependant, elle présente aussi de gros avantages :

- La démonstration classique est très obscure et il est difficile d'en extraire une idée générale, alors que la preuve par le théorème d'Artin-Verdier est assez naturelle.
- Les définitions des morphismes et des accouplements qui entrent en jeu sont très mystérieuses dans la démonstration classique, alors qu'elles sont plus claires dans cette nouvelle démonstration.
- On voit difficilement comment généraliser la preuve classique, alors que la preuve par le théorème d'Artin-Verdier est parfaitement généralisable et fournit une méthode pouvant être utilisée dans d'autres contextes. Par exemple, il est possible de prouver des analogues du théorème de Poitou-Tate pour les **corps de fonctions** (extensions finies séparables de $\mathbb{F}_q(t)$ pour un certain q, voir les sections 4 et 5 de [Izq13]), ou pour des corps comme $\mathbb{Q}_p(t)$ (voir le théorème 4.4 de [HS13]) ou $\mathbb{C}((t))(u)$. En effet, il suffit de prouver pour ces corps des "théorèmes d'Artin-Verdier", ce qui est nettement plus simple que pour les corps de nombres grâce à un théorème bien connu des géomètres, le **théorème de dualité de Poincaré**, puis de procéder de manière très similaire à celle des corps de nombres. De même, on peut remplacer le module discret fini M dans le théorème de Poitou-Tate par un tore (voir le théorème 4.1 de [HS13]) ou par une variété abélienne (voir la section 6 de [Izq13]).

Ainsi il semble intéressant de chercher un cadre axiomatique général dans lequel on pourrait prouver des analogues du théorème de Poitou-Tate. C'est l'une des directions sur lesquelles je vais travailler dans ma thèse.

Références

[Del77] P. Deligne. *Cohomologie étale.* Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 1/2, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier.

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

[Fu11] Lei Fu. *Etale cohomology theory*, volume 13 of *Nankai Tracts in Mathematics.* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2011.

[Hab78] Klaus Haberland. *Galois cohomology of algebraic number fields.* VEB Deutscher Verlag der Wissenschaften, Berlin, 1978. With two appendices by Helmut Koch and Thomas Zink.

[HS13] David Harari and Tamas Szamuely. Local-global principles for tori over p-adic function fields. 2013. Prepublication.

[Izq13] Diego Izquierdo. Le théorème de Poitou-Tate à partir du théorème d'Artin-Verdier. 2013. Mémoire sous la direction de David Harari.

[Kat86] Kazuya Kato. A Hasse principle for two-dimensional global fields. *J. Reine Angew. Math.*, 366 :142–183, 1986. With an appendix by Jean-Louis Colliot-Thélène.

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

[Mil06] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Poi67] G. Poitou. *Cohomologie galoisienne des modules finis*. Séminaire de l'Institut de Mathématiques de Lille, sous la direction de G. Poitou. Travaux et Recherches Mathématiques, No. 13. Dunod, Paris, 1967.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser77] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[SGA73] *Théorie des topos et cohomologie étale des schémas*. Lecture Notes in Mathematics, Vol. 269, 270, 305. Springer-Verlag, Berlin, 1972-1973. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat.

[Sha72] Stephen S. Shatz. *Profinite groups, arithmetic, and geometry*. Princeton University Press, Princeton, N.J., 1972. Annals of Mathematics Studies, No. 67.

[Tam94] Günter Tamme. *Introduction to étale cohomology*. Universitext. Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster.

[Tat63] John Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.