BULLETIN DE LA S. M. F.

LAURENT HERR

Sur la cohomologie galoisienne des corps p-adiques

Bulletin de la S. M. F., tome 126, n° 4 (1998), p. 563-600

<http://www.numdam.org/item?id=BSMF_1998__126_4_563_0>

Bull. Soc. math. France,
126, 1998, p. 563–600.

SUR LA COHOMOLOGIE GALOISIENNE DES CORPS p-ADIQUES

PAR LAURENT HERR (*)

RÉSUMÉ. — Ce travail fait suite à l'article de J.-M. Fontaine paru dans la *Grothendieck Festschrift*, où il construit une équivalence entre la catégorie des représentations p-adiques du groupe de Galois absolu G_K d'un corps local K d'inégale caractéristique $(0, p > 0)$ et une catégorie de modules sur un certain anneau, munis de deux opérateurs aux propriétés particulières. Nous donnons ici à l'aide de ces nouveaux objets une construction explicite des groupes de cohomologie galoisienne d'une représentation $\mathbb{Z}_p$-adique de p-torsion de G_K. Lorsque K est une extension finie de $\mathbb{Q}_p$, nous montrons ensuite comment on peut retrouver à partir de là les résultats classiques de Tate concernant ces groupes : la finitude et le calcul de la caractéristique d'Euler-Poincaré. Les méthodes utilisées semblent être plus simples que les arguments cohomologiques habituels, ne serait-ce que parce que l'on ne se sert pas de la théorie sophistiquée du corps de classe local et que tout est essentiellement explicite. Nous obtenons aussi au passage des résultats importants concernant la structure des modules associés aux représentations, ainsi qu'une filtration en trois crans sur leur cohomologie.

ABSTRACT. — ON GALOIS COHOMOLOGY OF p-ADIC FIELDS. — This work follows J.-M. Fontaine's paper in the *Grothendieck Festschrift*, where he constructs an equivalence between the category of $\mathbb{Z}_p$-adic representations of the absolute Galois group G_K of a local field K of mixed characteristic $(0, p > 0)$ and a category of modules over a certain ring, endowed with two operators satisfying special properties. We give here an explicit construction of the cohomology groups of a $\mathbb{Z}_p$-adic representation of G_K killed by a power of p, using these new objects. When K is a finite extension of $\mathbb{Q}_p$, we show then how one can find again Tate's classical results about these groups : the finiteness and the calculation of the Euler-Poincaré characteristic. The methods used seem to be rather simpler than the standard cohomological arguments because we don't need sophisticated theories like local class field theory and everything is essentially explicit. One gets also interesting information about the structure of the modules associated with representations and a 3-step filtration on their Galois cohomology.

(*) Texte reçu le 9 janvier 1998, révisé le 23 septembre 1998, accepté le 9 octobre 1998.
L. HERR, Laboratoire de Mathématiques Pures, Université Bordeaux 1, 351 cours de la Libération, 33405, Talence CEDEX (France).
E-mail : herr@math.u-bordeaux.fr.

Mots clés : cohomologie galoisienne, corps p-adiques.

Classification AMS : 11S25, 11S15, 11S31, 14F30.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037–9484/1998/563/$ 5.00

Introduction

Dans tout ce texte, K est un corps complet pour une valuation discrète, de caractéristique 0, à corps résiduel k parfait de caractéristique $p > 0$. On choisit une clôture séparable $\overline{K}$ de K, on note son corps résiduel $\bar{k}$ et on pose

$$G_K = \mathrm{Gal}(\overline{K}/K).$$

On appelle *représentation $\mathbb{Z}_p$-adique de G_K* la donnée d'un $\mathbb{Z}_p$-module V de type fini muni d'une action linéaire continue de G_K. Ces représentations forment une catégorie abélienne que l'on note

$$\mathbf{Rep}_{\mathbb{Z}_p}(G_K).$$

Si V est annulé par une puissance de p, on dit que la représentation est de *p-torsion*. Si V est un $\mathbb{F}_p$-espace vectoriel, on parle de *représentation mod p* de G_K. On note

$$\mathbf{Rep}_{p\text{-tor}}(G_K) \quad (\text{resp. } \mathbf{Rep}_{\mathbb{F}_p}(G_K))$$

la sous-catégorie pleine de $\mathbf{Rep}_{\mathbb{Z}_p}(G_K)$ formée des représentations de p-torsion (resp. mod p).

Soit V une représentation de p-torsion de G_K. On peut définir ses groupes de cohomologie $H^i(G_K, V)$. Rappelons les résultats classiques suivants :

THÉORÈME A (annulation de la cohomologie, [Se2, chap. II, prop. 12]). *Les groupes $H^i(G_K, V)$ sont nuls pour $i \geq 3$.*

THÉORÈME B (finitude de la cohomologie, *cf.* [Tat]). — *Lorsque k est* fini, *les groupes $H^i(G_K, V)$ le sont aussi et la caractéristique d'Euler-Poincaré vaut* :

$$\chi(V) = \prod_{1 \leq i \leq 2} \mathrm{card}\big(H^i(G_K, V)\big)^{(-1)^i} = p^{-[K:\mathbb{Q}_p]\,\mathrm{long}_{\mathbb{Z}_p}(V)}.$$

THÉORÈME C (dualité locale, *cf.* [Tat]). — *Soit $V^*(1) = \mathrm{Hom}(V, \mu_{p^\infty})$ le dual de V tordu à la Tate. Si k est* fini, *il existe un isomorphisme canonique de $H^2(G_K, \mu_{p^\infty})$ sur $\mathbb{Q}_p/\mathbb{Z}_p$. Pour $i \in \{0, 1, 2\}$, le cup-produit induit alors une dualité parfaite entre les groupes $H^i(G_K, V)$ et $H^{2-i}(G_K, V^*(1))$.*

Les démonstrations classiques de ces résultats (voir [Se2] ou [Mil]), qui utilisent de façon déterminante l'étude du groupe de Brauer, sont longues, difficiles et peu « explicites ». On se propose ici d'utiliser l'équivalence de catégorie décrite par J.-M. Fontaine [Fo1] dans la *Grothendieck Festschrift*,

entre représentions $\mathbb{Z}_p$-adiques de G_K et « Φ-Γ_K-module étales » pour associer à V un complexe canonique qui calcule sa cohomologie. On étudie en détail quelques propriétés de ce complexe, et on en déduit une démonstration « élémentaire » des théorèmes A et B. On obtient également une décomposition canonique des groupes de cohomologie $H^i(G_K, V)$. Nous montrerons dans une publication ultérieure comment on peut aussi retrouver le théorème C par ce type de techniques.

Lorsque le corps résiduel de K est fini, on peut généraliser les résultats précédents à la cohomologie continue des représentations $\mathbb{Z}_p$-adiques quelconques, ou même à celle des *représentations p-adiques de* G_K, *i.e.* des $\mathbb{Q}_p$-espaces vectoriels de dimension finie munis d'une action linéaire continue de G_K, de la façon suivante.

Rappelons qu'on dit qu'un système projectif $(A_n, \pi_n)_{n\in\mathbb{N}}$ vérifie la *condition de Mittag-Leffler* si, pour tout entier naturel n, l'image des applications de transition $A_{n+m} \to A_n$ est constante pour m assez grand.

Si T est une représentation $\mathbb{Z}_p$-adique de G_K et i un entier naturel, le théorème de finitude B entraîne alors que le système projectif des $H^i(G_K, T/p^nT)$ vérifie la condition de Mittag-Leffler et de ce fait l'application naturelle

$$H^i(G_K, T) \longrightarrow \varprojlim_{n\geq 1} H^i(G_K, T/p^nT)$$

est un isomorphisme. De plus, si V est une représentation p-adique de G_K et T un réseau de V stable par l'action de G_K, alors, pour tout entier naturel i, on a :

$$H^i(G_K, V) \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i(G_K, T).$$

Par passage à la limite et extension des scalaires, on déduit donc des théorèmes A à C, le résultat suivant :

THÉORÈME. — *On suppose k fini. Soit T une représentation $\mathbb{Z}_p$-adique de G_K. Alors ses groupes de cohomologie continue $H^i(G_K, T)$ sont des $\mathbb{Z}_p$-module de type fini, nuls pour $i \geq 3$ et si T est sans torsion, on a la relation :*

$$\sum_{i\in\mathbb{N}} (-1)^i \operatorname{rang}_{\mathbb{Z}_p} H^i(G_K, T) = -[K : \mathbb{Q}_p] \operatorname{rang}_{\mathbb{Z}_p} T.$$

De plus, il existe un isomorphisme canonique de $H^2(G_K, \mathbb{Z}_p(1))$ sur $\mathbb{Z}_p$ et, si $T^*(1)$ désigne le dual de T tensorisé par $\mathbb{Z}_p(1)$, alors, pour $i \in \{0, 1, 2\}$, le cup-produit induit une dualité parfaite entre les $\mathbb{Z}_p$-modules $H^i(G_K, T)$ et $H^{2-i}(G_K, T^*(1))$.

Si V est une représentation p-adique de G_K, on a les résultats analogues en remplaçant $\mathbb{Z}_p$ par $\mathbb{Q}_p$.

Voici le plan de cet article :

- § 1 : on rappelle la construction de Fontaine qui permet d'associer à toute représentation de p-torsion V de G_K un « Φ-Γ_K-module étale de torsion M sur $\mathcal{O}_{\mathcal{E}(K)}$ » ;
- § 2 : on construit en utilisant M un complexe canonique de longueur 2 qui calcule la cohomologie galoisienne de V, ce qui prouve le théorème A ;
- § 3 : on construit un inverse à gauche ψ_M du Frobenius ϕ_M agissant sur M et on étudie quelques unes de ses propriétés ;
- § 4 : on montre comment retrouver le théorème B à l'aide des résultats du paragraphe précédent ;
- § 5 : on utilise des calculs de ramification pour prouver un résultat énoncé au paragraphe 3 qui est le cœur technique du théorème sur la structure du noyau de ψ_M.

Cet article est une version remaniée par endroits, d'après des suggestions de J.-M. Fontaine, de la thèse de l'auteur sous sa direction. Plus précisément, la partie 3.3 donne une présentation plus agréable de la structure du noyau de l'opérateur ψ_M, entre autre par un usage plus poussé de la notion de « réseau » ; le § 5 généralise un peu l'étude initiale de l'action du groupe Γ_K sur le quotient d'un corps de séries formelles de caractéristique p par les puissances p-ièmes. Cet article a probablement gagné ainsi en clarté et en concision.

Je tiens donc à terminer cette introduction en remerciant chaleureusement J.-M. Fontaine d'avoir eu la patience de guider mes pas dans ce travail, qui, sans lui, n'aurait sans doute pas vu le jour.

1. Préliminaires

1.1. Construction de quelques anneaux.

Pour les détails on renvoie le lecteur à [Fo1, A3.1–3.2].

1.1.1. Le corps FrR.

1.1.1.1. Définition. — On note C le complété de $\overline{K}$ pour la topologie p-adique, v_C la valuation de C normalisée par $v_C(p) = 1$ et $\mathrm{Fr}\, R$ l'ensemble des suites $(x^{(n)})_{n\in\mathbb{N}}$ de C telles que, pour tout $n \in \mathbb{N}$,

$$(x^{(n+1)})^p = x^{(n)}.$$

On munit $\mathrm{Fr}\, R$ d'une addition et d'une multiplication en posant pour tout $x = (x^{(n)})_{n\in\mathbb{N}}$ et tout $y = (y^{(n)})_{n\in\mathbb{N}}$ dans $\mathrm{Fr}\, R$:

$$xy = (x^{(n)}y^{(n)})_{n\in\mathbb{N}}, \quad x + y = \Big(\lim_{m\to+\infty} (x^{(m+n)} + y^{(m+n)})^{p^m}\Big)_{n\in\mathbb{N}}.$$

On obtient alors un corps algébriquement clos de caractéristique p, complet pour la valuation v définie par

$$v(x) = v_C(x^{(0)})$$

et son corps résiduel s'identifie à $\bar{k}$ de la façon suivante : à $x \in \bar{k}$, on associe l'élément $([x]^{p^{-n}})_{n\in\mathbb{N}}$ de Fr R, où $[x]$ est le relèvement de Teichmüller de x dans C. On note R l'anneau de la valuation. Le groupe $G_K = \mathrm{Gal}(\overline{K}/K)$ opère continûment sur Fr R.

1.1.1.2. Lien avec le corps des normes. — Dans tout cet article, sauf dans le § 5, K_∞ désigne la $\mathbb{Z}_p$-extension cyclotomique de K contenue dans $\overline{K}$; son corps résiduel k_∞ est une extension finie de k. Pour tout $n \in \mathbb{N}$, on note $K^{(n)}$ l'unique extension de K de degré p^n contenue dans K_∞. Pour une extension de corps quelconque L/T, on désigne par $\mathcal{E}_{L/T}$ l'ensemble ordonné filtrant des extensions finies de T contenues dans L.

Pour toute extension finie L de K_∞, on peut définir le *corps des normes* $E_K(L)$ de L/K (pour toute la théorie, on renvoie à [Win]). Rappelons qu'en tant qu'ensemble,

$$E_K(L) = \varprojlim_{T\in\mathcal{E}_{L/K}} T,$$

les applications de transition étant les normes. Pour $x = (x_T)_{T\in\mathcal{E}_{L/K}}$ et $y = (y_T)\mathcal{E}_{L/K} \in E_K(L)$, on définit la somme et le produit par

$$xy = (x_T y_T)_{T\in\mathcal{E}_{L/K}},$$

$$x + y = \left(\varprojlim_{T'\in\mathcal{E}_{L/T}} N_{T'/T}(x_{T'} + y_{T'})\right)_{T\in\mathcal{E}_{L/K}},$$

la limite étant prise suivant le filtre des sections de $\mathcal{E}_{L/T}$. Alors, $E_K(L)$ est un corps de caractéristique p, complet pour la valuation discrète donnée par

$$v(x) = v_C(x_K)$$

et son corps résiduel s'identifie à celui de L.

Cette construction est en fait fonctorielle et donne, par passage à la limite inductive, une équivalence entre la catégorie des extensions algébriques de K_∞ et celle des extensions séparables de $E_K(K_\infty)$. Le corps

$$E_K(\overline{K}) = \varinjlim_{L\in\mathcal{E}_{\overline{K}/K_\infty}} E_K(L)$$

est donc une clôture séparable de $E_K(K_\infty)$. Le groupe G_K opère de façon continue sur $E_K(\overline{K})$ par fonctorialité; cette action permet d'identifier $\mathrm{Gal}(E^{\mathrm{sep}}/E_K(K_\infty))$ à $\mathrm{Gal}(\overline{K}/K_\infty)$ et, pour tout $L \in \mathcal{E}_{\overline{K}/K_\infty}$, on a :

$$E_K(L) = \big(E_K(\overline{K})\big)^{\mathrm{Gal}(\overline{K}/L)}.$$

Il existe de plus un plongement continu et G_K-équivariant j_K de $E_K(\overline{K})$ dans $\mathrm{Fr}\, R$ qui est défini de la façon suivante : soient L une extension finie de K_∞ contenue dans $\overline{K}$ et L^{mr} l'extension maximale modérément ramifiée de K dans L; pour tout $r \in \mathbb{N}$, on note $\mathcal{E}_r(L)$ l'ensemble des extension finies T de L^{mr} contenues dans L et telles que p^r divise $[T : L^{\mathrm{mr}}]$; alors, si $x = (x_T)_{T \in \mathcal{E}_{L/K}}$ est dans $E_K(L)$, la famille

$$\big(x_T^{p^{-r}[T:L^{mr}]}\big)_{T \in \mathcal{E}_r(L)}$$

converge suivant le filtre des sections de $\mathcal{E}_r(L)$ vers un élément $j_K(x)^{(r)}$ de C pour tout $r \in \mathbb{N}$ et

$$j_K(x) = (j_K(x)^{(r)})_{r \in \mathbb{N}}$$

est dans $\mathrm{Fr}\, R$. On montre ensuite que l'application

$$j_K : E_K(\overline{K}) \longrightarrow \mathrm{Fr}\, R$$

ainsi construite convient et que son image est dense dans $\mathrm{Fr}\, R$ (*cf.* [Win, cor. 4.3.4]). On décrira ce plongement d'une autre manière au paragraphe suivant.

1.1.2. Les anneaux $\mathcal{O}_{\mathcal{E}(\boldsymbol{K})}$ et $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$.

1.1.2.1. Construction. — Pour toute $\mathbb{F}_p$-algèbre A, on note $W(A)$ l'anneau des vecteurs de Witt à coefficients dans A. On pose

$$W = W(k)$$

et on note K_0 le corps des fractions de W. L'anneau $W(\mathrm{Fr}\, R)$ est muni naturellement d'un Frobenius σ et d'une action continue de G_{K_0}, qui commutent entre eux. Soit

$$[\epsilon] = \big(\epsilon = (\epsilon^{(n)})_{n \in \mathbb{N}}, 0, 0, \ldots, 0, \ldots\big)$$

un élément de $W(\operatorname{Fr} R)$ tel que $\epsilon^{(0)} = 1$ et $\epsilon^{(1)} \neq 1$. Notons $\mathcal{E}_0'$ le corps des fractions du séparé complété, pour la topologie p-adique, de l'anneau

$$W\big([[\epsilon]-1)\big) := W\big[\big[[\epsilon]-1\big]\big]\Big[\frac{1}{[\epsilon]-1}\Big].$$

Il s'identifie à un sous-corps de $W(\operatorname{Fr} R)$, stable par le Frobenius et l'action de G_{K_0} car on a les relations :

$$\sigma\big([\epsilon]\big) = [\epsilon]^p, \quad \forall g \in G_{K_0}, \quad g\big([\epsilon]\big) = [\epsilon]^{\chi(g)}.$$

où $\chi : G_{K_0} \longrightarrow \mathbb{Z}_p^*$ désigne le caractère cyclotomique. On en déduit que le groupe G_{K_0} opère continûment sur le corps $\mathcal{E}_0'$ à travers le quotient

$$\operatorname{Gal}\Big(\bigcup_{n\in\mathbb{N}} K_0(\sqrt[p^n]{1})/K_0\Big)$$

qui est isomorphe à un produit de $\mathbb{Z}_p$ par un groupe fini Γ_{tor}, cyclique d'ordre $p-1$ si $p \neq 2$ (resp. d'ordre 2 si $p = 2$). On pose

$$\mathcal{E}_0 = (\mathcal{E}_0')^{\Gamma_{\mathrm{tor}}}.$$

C'est un corps valué complet dont l'anneau des entiers $\mathcal{O}_{\mathcal{E}_0}$ est la complétion p-adique de $W((\pi_0))$ où

$$\pi_0 = \operatorname{Tr}_{\mathcal{E}_0'/\mathcal{E}_0}\big([\epsilon]-1\big)$$

(*cf.* [Fo1, A.3.2]). Si $(K_0)_\infty$ désigne la $\mathbb{Z}_p$-extension cyclotomique de K_0 contenue dans $\overline{K}$, le corps résiduel E_0 de $\mathcal{E}_0$ est le corps des normes de l'extension $(K_0)_\infty/K_0$.

On considère alors l'anneau de valuation discrète $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$ qui est la réunion des sous-$\mathcal{O}_{\mathcal{E}_0}$-algèbres étales de $W(\operatorname{Fr} R)$: son corps des fractions $\mathcal{E}^{\mathrm{nr}}$ est la réunion des extensions finies non ramifiées de $\mathcal{E}_0$ contenues dans $W(\operatorname{Fr} R)[1/p]$; son corps résiduel, qui s'identifie à un sous-corps de $\operatorname{Fr} R$, est une clôture séparable E^{sep} de E_0 . Les anneaux $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$, $\mathcal{E}^{\mathrm{nr}}$ et E^{sep} sont stables par σ et par l'action de G_{K_0}.

On pose

$$\mathcal{E}(K) = (\mathcal{E}^{\mathrm{nr}})^{\operatorname{Gal}(\overline{K}/K_\infty)}.$$

C'est un corps valué complet, dont l'anneau des entiers est

$$\mathcal{O}_{\mathcal{E}(K)} = (\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}})^{\operatorname{Gal}(\overline{K}/K_\infty)} ;$$

l'idéal maximal de $\mathcal{O}_{\mathcal{E}(K)}$ est engendré par p; son corps résiduel E_K s'identifie au corps des normes de l'extension K_∞/K et est une extension séparable de E_0 de degré

$$d_K = \big[K_\infty : K \cap (K_0)_\infty\big].$$

Les anneaux $\mathcal{E}(K)$, $\mathcal{O}_{\mathcal{E}(K)}$ et E_K sont stables par le Frobenius σ et munis d'une action continue de $\Gamma_K = \mathrm{Gal}(K_\infty/K)$. De plus, Γ_K opère trivialement sur le sous-corps k de E_K, mais ce n'est en général pas le cas pour le corps résiduel k_∞.

On pose

$$G_{E_K} = \mathrm{Gal}(E^{\mathrm{sep}}/E_K) = \mathrm{Gal}\big(\mathcal{E}^{\mathrm{nr}}/\mathcal{E}(K)\big)\,;$$

il s'identifie à $\mathrm{Gal}(\overline{K}/K_\infty)$, sous-groupe fermé invariant de G_K.

Il est important de noter que ces constructions ne dépendent pas du choix de ϵ. De plus, les corps E_0, E_K et E^{sep} se plongent de façon naturelle dans $\mathrm{Fr}\,R$ et ils s'identifient alors aux images par l'application j_{K_0} de $E_{K_0}((K_0)_\infty)$, $E_K(K_\infty)$ et $E_K(\overline{K})$.

1.1.2.2. Quelques précisions sur l'action de Galois. — Si t est un relèvement dans $\mathcal{O}_{\mathcal{E}(K)}$ d'une uniformisante de E_K, alors $\mathcal{O}_{\mathcal{E}(K)}$ s'identifie à la complétion p-adique de $W(k_\infty)[[t]][1/t]$. Mais, en général, il n'est pas possible de choisir t pour que $W(k_\infty)[[t]]$ soit stable à la fois par l'action de Γ_K et par celle de σ : en effet, si c'était le cas, la représentation obtenue en induisant de K à K_0 la représentation triviale serait de hauteur finie; elle deviendrait donc cristalline sur l'un des $(K_0)^{(n)}$ d'après un résultat de N. Wach (*cf.* [Wac, § A.5]) et cela impliquerait que K est non ramifié sur $(K_0)^{(n)}$! Un tel choix est toutefois possible lorsque $d_K = [k_\infty : k]$, c'est-à-dire lorsque K est contenu dans une extension non ramifiée de $(K_0)_\infty$, auquel cas on peut prendre pour t l'élément π_0 défini plus haut. On peut même préciser un peu plus cela :

LEMME 1.1. — *Pour tout $g \in G_K$, l'élément $g(\pi_0)/\pi_0$ est une unité de l'anneau $W[[\pi_0]]$. Si l'extension K_∞/K est totalement ramifiée et si π est une uniformisante de E_K, alors pour tout $g \in G_K$, l'élément $g(\pi)/\pi$ est une unité fondamentale de E_K, c'est-à-dire un élément de l'anneau des entiers congru à 1 modulo l'idéal maximal.*

Preuve. — Soit $\mathcal{O}_C$ le séparé complété pour la topologie p-adique de l'anneau des entiers de $\overline{K}$ et soit $\theta : W(R) \to \mathcal{O}_C$ l'homomorphisme de W-algèbres introduit par Fontaine (*cf.* [Fo2]). On voit que le noyau de la restriction de θ à $W[[\pi_0]]$ est l'idéal engendré par π_0. Comme θ est G_K-équivariante, pour tout $g \in \Gamma_K$, les éléments π_0 et $g(\pi_0)$ engendrent le même idéal de $W[[\pi_0]]$.

Quant à la deuxième assertion, elle provient simplement du fait que si K_∞/K est totalement ramifiée, le corps résiduel de E_K est k, sur lequel G_K opère trivialement. □

1.1.2.3. « Topologie naturelle » sur un $\mathcal{O}_{\mathcal{E}_0}$-module de longueur finie. — Soient X une indéterminée sur W et M un $W((X))$-module de longueur finie. La *topologie naturelle* sur M est celle dont une base de voisinages ouverts de 0 est formée par les sous-$W[[X]]$-modules de type fini contenant un système générateur de M sur $W((X))$. Si l'on fixe un tel sous-$W[[X]]$-module N, alors on peut aussi prendre comme base de voisinages ouverts de 0 pour cette topologie les parties de la forme $X^n N$, pour n parcourant $\mathbb{N}$.

Soit M un $\mathcal{O}_{\mathcal{E}_0}$-module de longueur finie. Comme M est alors tué par une puissance de p, on peut le voir comme un $W((\pi_0))$-module de longueur finie et donc le munir de la topologie naturelle définie plus haut.

1.2. Lien avec les représentations $\mathbb{Z}_p$-adiques de G_K : l'équivalence de catégorie D_K.

Rappelons que, si Γ est un sous-groupe ouvert non trivial de Γ_K, Fontaine appelle Φ-Γ-*module* sur $\mathcal{O}_{\mathcal{E}(K)}$, la donné d'un $\mathcal{O}_{\mathcal{E}(K)}$-module M muni :

1) d'un opérateur σ-semi-linéaire, le « Frobenius » $\phi = \phi_M : M \to M$,

2) d'une action Γ-semi-linéaire continue du groupe Γ qui commute avec celle de ϕ.

On dit que M est un Φ-Γ-*module étale de torsion* si, en tant que $\mathcal{O}_{\mathcal{E}(K)}$-module, il est de longueur finie et engendré par l'image de ϕ.

Les Φ-Γ-modules étales de torsion sur $\mathcal{O}_{\mathcal{E}(K)}$ forment une catégorie abélienne, les flèches étant les morphismes $\mathcal{O}_{\mathcal{E}(K)}$-linéaires qui commutent à ϕ et à l'action de Γ. On note

$$\mathbf{\Phi\Gamma M}^{\text{et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}(K)}}$$

la catégorie des Φ-Γ_K-modules étales de torsion .

On peut associer à toute représentation $V \in \mathbf{Rep}_{p\text{-tor}}(G_K)$, le $\mathcal{O}_{\mathcal{E}(K)}$-module :

$$D_K(V) = \left(\mathcal{O}_{\mathcal{E}^{\text{nr}}} \otimes_{\mathbb{Z}_p} V\right)^{G_{E_K}}.$$

Il est muni d'une action naturelle de $\Gamma_K = G_K/G_{E_K}$ et on considère l'action de ϕ induite par celle du Frobenius σ sur $\mathcal{O}_{\mathcal{E}^{\text{nr}}}$; c'est alors un Φ-Γ_K-module étale de torsion.

Inversement, à tout Φ-Γ_K-module étale de torsion M sur $\mathcal{O}_{\mathcal{E}(K)}$, on peut faire correspondre la représentation de p-torsion de G_K suivante :

$$V_K(M) = \left(\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \otimes_{\mathcal{O}_{\mathcal{E}(K)}} M\right)_{\sigma\otimes\phi_M=1}.$$

Ces deux constructions définissent des foncteurs additifs exacts et Fontaine a montré que l'on a :

THÉORÈME 1.2 (*cf.* [Fo1, A.1.2.4–A.1.2.6]). — *Le foncteur D_K est une équivalence de catégorie de quasi-inverse V_K entre*

$$\mathbf{Rep}_{p\text{-tor}}(G_K) \quad \textit{et} \quad \mathbf{\Phi\Gamma M}^{\text{et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}(K)}}.$$

De plus, les facteurs invariants sur $\mathbb{Z}_p$ d'une représentation de p-torsion V de G_K coïncident avec ceux de $D_K(V)$ sur $\mathcal{O}_{\mathcal{E}(K)}$ (à des unités près).

2. Les complexes $C_{\phi,\gamma}$

On fixe une fois pour toutes un générateur topologique noté γ du groupe Γ_K et on pose

$$\tau = \gamma - 1, \quad \rho = \phi - 1.$$

L'objectif de cette partie est de prouver le résultat suivant qui est à la base de tout cet article :

THÉORÈME 2.1. — *Soit V une représentation de p-torsion de G_K. Alors, pour tout entier naturel i, le groupe $H^i(G_K, V)$ est isomorphe au i-ème groupe de cohomologie du complexe $C_{\phi,\gamma}(D_K(V))$ (où le premier terme est en degré -1) :*

$$\begin{aligned} 0 \to D_K(V) &\longrightarrow D_K(V) \oplus D_K(V) \longrightarrow D_K(V) \longrightarrow 0 \to 0 \cdots, \\ x &\longmapsto (\rho(x), \tau(x)) \\ & \qquad\qquad (y,z) \longmapsto \tau(y) - \rho(z). \end{aligned}$$

En particulier, cela prouve que pour tout $i \geq 3$, les groupes $H^i(G_K, V)$ sont nuls. D'où une preuve simple du théorème A.

REMARQUE. — Si γ' est un autre générateur topologique de Γ_K, on dispose d'un *isomorphisme canonique* de complexes

$$C_{\phi,\gamma}\left(D_K(V)\right) \longrightarrow C_{\phi,\gamma'}\left(D_K(V)\right);$$

l'idéal de $\mathbb{Z}_p[[\Gamma_K]]$ engendré par $\tau' = \gamma' - 1$ est le même que celui engendré par τ ; si l'on pose $\tau' = \delta\,\tau$, l'isomorphisme est donné par les applications $x \mapsto x$ en degré 0, $(y,z) \mapsto (y, \delta(z))$ en degré 1 et $t \mapsto \delta(t)$ en degré 2.

L'idée de la *démonstration de ce théorème* est la suivante : le foncteur D_K se prolonge en une équivalence entre la catégorie des G_K-modules

discrets de p-torsion et celle, notée $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}}(K)}$, formée par les limites inductives de Φ-Γ_K-modules étales de p-torsion sur $\mathcal{O}_{\mathcal{E}(K)}$. Ces catégories ont assez d'injectifs, contrairement à $\mathbf{\Phi\Gamma M}^{\text{et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}}(K)}$. Or calculer la cohomologie des G_K-modules discrets de p-torsion revient à dériver dans la catégorie dont ils sont les objets, le foncteur $H^0(G_K, \cdot)$. Mais pour un G_K-module discret de p-torsion V, on a :

$$\big(D_K(V)\big)_{\phi=1,\gamma=1} \simeq V^{G_K}.$$

Il s'agit donc de dériver dans la catégorie $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}}(K)}$ le foncteur qui à un objet M associe le groupe de ses éléments fixes par ϕ et γ.

Rappelons qu'un foncteur F entre deux catégories abéliennes $\mathcal{C}$ et $\mathcal{C}'$ est dit *effaçable* si pour tout objet M de $\mathcal{C}$ et tout $x \in F(M)$ il existe dans $\mathcal{C}$ une injection u de M dans un objet N tel que $F(u)(x) = 0$ dans $F(N)$.

On considère alors le foncteur $\mathcal{C}_{\phi,\gamma}$ de $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}}(K)}$ dans la catégorie des complexes de groupes abéliens, qui à un Φ-Γ_K-module ind-étale M associe le complexe $\mathcal{C}_{\phi,\gamma}(M)$:

$$\begin{aligned} 0 \to M \longrightarrow M \oplus M \longrightarrow M \longrightarrow 0 \to 0 \cdots, \\ x \longmapsto (\rho(x), \tau(x)), \\ (y,z) \longmapsto \tau(y) - \rho(z). \end{aligned}$$

Ce foncteur est additif, exact et fidèle. Il définit donc un foncteur cohomologique $(\mathcal{H}^i = H^i \circ \mathcal{C}_{\phi,\gamma}, \delta^i)_{i\in\mathbb{N}}$ de $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}}(K)}$ dans la catégorie des groupes abéliens.

Comme en degré 0 il coïncide avec la cohomologie galoisienne de G_K *via* D_K, il suffit de montrer qu'il est effaçable en degré plus élevé (*cf.* [Poi, cor. p. 65]).

2.1. Preuve de l'effaçabilité.

Elle découle du lemme suivant :

LEMME 2.2. — *Soient M un objet de $\mathbf{\Phi\Gamma M}^{\text{et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}}(K)}$ et x un élément de M. Alors, M se plonge dans un Φ-Γ_K-module étale de torsion N_x tel que $x \in \rho(N_x)$.*

Supposons en effet le lemme démontré. Il suffit de vérifier l'effaçabilité du foncteur $\mathcal{H}^i$ en degrés 1 et 2.

Soit M un objet de $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}}(K)}$: il est réunion de ses sous-Φ-Γ_K-modules étales de p-torsion. En degré 2, si $x \in M$, par le lemme 2.2, M

se plonge dans un objet N_x de $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}(K)}}$ tel que $x \in \rho(N_x)$, et x s'envoie sur 0 dans $\mathcal{H}^2(N_x)$.

En degré 1, soient $y, z \in M$ tels que $\tau(y) = \rho(z)$. Par le lemme 2.2, M se plonge dans un objet N_y de $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}(K)}}$ tel qu'il existe $x \in N_y$ vérifiant $\rho(x) = y$. Soit s un entier tel que

$$p^s x = p^s z = 0.$$

Notons alors $N_{y,z}$ la somme directe de N_y et du $\mathcal{O}_{\mathcal{E}(K)}/p^s\mathcal{O}_{\mathcal{E}(K)}$-module libre de rang 1 engendré par un élément v et prolongeons ϕ_{N_y} et γ à $N_{y,z}$ en posant :

$$\phi(v) = v, \quad \gamma(v) = v + \tau(x) - z.$$

On vérifie que $\phi(\gamma(v)) = \gamma(\phi(v))$ et on voit que le fait que $\tau(v) \in N_y$ implique que l'action de γ se prolonge en une action semi-linéaire et continue de Γ_K sur $N_{y,z}$ qui devient ainsi un objet de $\mathbf{\Phi\Gamma M}^{\text{ind-et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}(K)}}$. Par construction, on a :

$$y = \rho(x - v), \quad z = \tau(x - v).$$

On en déduit bien que (y, z) s'envoie sur 0 dans le groupe $\mathcal{H}^1(N_{y,z})$.

Pour prouver le lemme 2.2, il nous faut d'abord étudier de plus près l'action de ϕ sur M.

2.2. Réseaux dans des Φ-Γ_K-modules sur $\mathcal{O}_{\mathcal{E}_0}$.

DÉFINITION 2.3. — *Soient X une indéterminée et N un $W((X))$-module de longueur finie. On appelle X-*réseau de N *tout sous-$W[[X]]$-module de type fini Λ de N qui engendre N en tant que $W((X))$-module.*

Remarquons qu'il revient au même de parler de $\mathcal{O}_{\mathcal{E}_0}$-module de longueur finie ou de $W((\pi_0))$-module de longueur finie.

PROPOSITION 2.4. — *Soit M un Φ-Γ_K-module sur $\mathcal{O}_{\mathcal{E}_0}$, de longueur finie comme $\mathcal{O}_{\mathcal{E}_0}$-module. On a les propriétés suivantes :*

1) *M contient un π_0-réseau stable par ϕ et Γ_K, sur lequel ρ est bijective.*

2) *Pour tout $x \in M$, il existe un entier naturel r et un élément y de M tels que :*

$$\tau^r(x) = \rho(y).$$

Preuve.

1) On commence par construire un π_0-réseau stable par ϕ sur lequel ρ est bijectif. On reprend essentiellement la preuve de [Fo1, B1, Lemme 1.4.3].

Soient $n \geq 1$ un entier tel que p^n annule M et $(e_i)_{1\leq i\leq d}$ un système générateur de M sur $W((\pi_0))$; il existe alors une matrice $((a_{i,j}))_{1\leq i,j\leq d}$ à coefficients dans $W((\pi_0))$ telle que pour tout i dans $\{1,\ldots,d\}$:

$$\phi(e_i) = \sum_{1\leq j\leq d} a_{j,i}e_j.$$

Choisissons un entier $s \geq 0$ tel que, pour tous i, j :

$$\pi_0^s\, a_{i,j} \in \pi_0^{p^{n-1}} W[[\pi_0]] + p^n W((\pi_0)).$$

Soit alors $r \in \mathbb{N}$ tel que $p^{n-1}(p-1)r \geq s$. Comme $\sigma(\pi_0) \equiv \pi_0^p (\mathrm{mod}\ p)$, on a $\sigma(\pi_0^{p^{n-1}}) \equiv \pi_0^{p^n} (\mathrm{mod}\ p^n)$. Donc, pour tout i :

$$\phi(\pi_0^{p^{n-1}r} e_i) = \sum_{j=1}^{d} (\pi_0^{p^{n-1}(p-1)r} a_{j,i})(\pi_0^{p^{n-1}r} e_j).$$

Pour tout i, posons

$$f_i = \pi_0^{p^{n-1}r} e_i$$

et soit $\mathcal{R}$ le sous-$W[[\pi_0]]$-module de M engendré par les f_i. D'après la formule précédente, $\mathcal{R}$ est stable par ϕ. Comme les f_i engendrent M sur $W((\pi_0))$, on voit que $\mathcal{R}$ est un π_0-réseau de M stable par ϕ.

On va maintenant montrer que :

$$\forall x \in \mathcal{R}, \quad \lim_{r\to+\infty} \phi^r(x) = 0.$$

Si $x \in \mathcal{R}$ s'écrit

$$x = \sum_{1\leq i\leq d} x_i f_i,$$

on a :

$$\phi(x) = \sum_{j=1}^{d} \Big(\sum_{i=1}^{d} \sigma(x_i)(\pi_0^{p^{n-1}(p-1)r} a_{j,i}) \Big) f_j.$$

On en déduit que $\phi(x) \in \pi_0^{p^{n-1}} \mathcal{R}$. De même, si $t \in \mathbb{N}$ et si $y \in \pi_0^{tp^{n-1}} \mathcal{R}$, alors $\phi(y) \in \pi_0^{tp^n} \phi(\mathcal{R}) \subset \pi_0^{(1+tp)p^{n-1}} \mathcal{R}$. Donc :

$$\lim_{r\to+\infty} \phi^r(x) = 0.$$

Par conséquent, $\sum_{n\in\mathbb{N}}(-\phi^n)(x)$ converge dans $\mathcal{R}$. L'application ρ est donc inversible sur $\mathcal{R}$ et on a :

$$\rho^{-1} = \sum_{r\in\mathbb{N}} (-\phi^r).$$

Le fait que M soit un $W((\pi_0))$-module de longueur finie implique que $\mathcal{R}$ est un voisinage ouvert de 0 dans M.

Soit $x \in \mathcal{R}$. La continuité de l'action de Γ_K sur M implique que la suite des $\gamma^{p^r}(x) - x$ tend vers 0 dans M donc que $\gamma^{p^r}(x) - x$ et aussi $\gamma^{p^r}(x)$ sont dans $\mathcal{R}$ pour r assez grand. Soient $x_1, x_2, \ldots, x_d$ des générateurs de $\mathcal{R}$ sur $W[[\pi_0]]$ et soit r un entier ≥ 1 tel que les $\gamma^{p^r}(x_i)$ sont dans $\mathcal{R}$. En utilisant le fait que l'anneau $W[[\pi_0]]$ est stable par Γ_K, on voit que

$$\mathcal{R}' = \sum_{0 \leq t < p^r} \gamma^t(\mathcal{R})$$

l'est aussi. C'est encore un π_0-réseau de M stable par ϕ. De plus, pour tout $x \in \mathcal{R}'$, la suite des $\phi^r(x)$ tend vers 0, donc ρ est encore inversible sur $\mathcal{R}'$.

2) Comme le réseau $\mathcal{R}'$ que l'on vient de construire est un voisinage ouvert de 0 dans M sur lequel ρ est inversible, il suffit de prouver que, pour tout $x \in M$, la suite des $\tau^r(x)$ tend vers 0 lorsque r tend vers $+\infty$, ce qui résulte de la continuité de l'action de Γ_K sur M. □

2.3. Preuve du lemme 2.2.

Soient M un objet de $\mathbf{\Phi\Gamma M}^{\text{et},p\text{-tor}}_{\mathcal{O}_{\mathcal{E}(K)}}$ et x un élément de M. Comme $\mathcal{O}_{\mathcal{E}(K)}$ est un $\mathcal{O}_{\mathcal{E}_0}$-module de type fini et Γ_K un sous-groupe ouvert de Γ_{K_0}, on peut voir M comme un Φ-Γ_K-module de torsion sur $\mathcal{O}_{\mathcal{E}_0}$. D'après la proposition 2.4, on peut trouver un entier naturel r tel que

$$(\gamma - 1)^r(x) \in \rho(M).$$

Si $r = 0$, il n'y a rien à prouver. Si $r \geq 1$, on choisit $t_0 \in M$ tel que $\tau^r(x) = \rho(t_0)$. Soit n un entier tel que p^n annule M. On considère alors la somme directe N_x de M et du $\mathcal{O}_{\mathcal{E}(K)}/p^n\mathcal{O}_{\mathcal{E}(K)}$-module libre de rang r engendré par des éléments $t_1, \ldots, t_r$. On prolonge l'action de ϕ et de γ à N_x en posant pour tout $i \in \{1, \ldots, r\}$:

$$\phi(t_i) = t_i + \tau^{r-i}(x), \quad \gamma(t_i) = t_i + t_{i-1}.$$

Par construction, on a

$$\rho(t_r) = x$$

et ϕ commute avec γ : en effet, comme c'est le cas sur M, il suffit, par semi-linéarité, de remarquer que pour tout $i \in \{1, \ldots, r\}$, on a :

$$\begin{aligned} \phi\big(\gamma(t_i)\big) &= \phi(t_i) + \phi(t_{i-1}) \\ &= t_i + t_{i-1} + \tau\big(\tau^{r-i}(x)\big) + \tau^{r-i}(x) \\ &= \gamma\big(t_i + \tau^{r-i}(x)\big) = \gamma\big(\phi(t_i)\big). \end{aligned}$$

De plus, il résulte facilement de ce que $\tau^r(t_i) \in M$ pour tout i que l'action de γ se prolonge en une action linéaire et continue de Γ_K sur N_x.

Le $\mathcal{O}_{\mathcal{E}(K)}$-module de longueur finie N_x est ainsi muni d'une structure de Φ-Γ_K-module sur $\mathcal{O}_{\mathcal{E}(K)}$. Le fait qu'il est étale se déduit immédiatement du fait que M l'est. □

3. L'opérateur ψ

À la différence du théorème A, le complexe $\mathcal{C}_{\phi,\gamma}(D_K(V))$ ne semble pas donner une preuve directe simple du théorème B. Dans cette partie, on introduit un inverse à gauche additif ψ du Frobenius ϕ de $D_K(V)$; il permettra au paragraphe suivant de donner un complexe quasi-isomorphe à $\mathcal{C}_{\phi,\gamma}(D_K(V))$, dont on pourra dévisser de façon naturelle la cohomologie pour prouver le théorème B. Dans cette décomposition, la structure du noyau de ψ joue un rôle fondamental et constitue le résultat essentiel de cette partie (th. 3.8).

3.1. Définition.

3.1.1. Cas de l'anneau $\mathcal{O}_{\mathcal{E}(K)}$. — L'extension $\mathcal{E}^{\mathrm{nr}}/\sigma(\mathcal{E}^{\mathrm{nr}})$ est de degré p, de même que l'extension résiduelle qui est purement inséparable. Ceci implique que l'on a l'inclusion :

$$\mathrm{Tr}_{\mathcal{E}^{\mathrm{nr}}/\sigma(\mathcal{E}^{\mathrm{nr}})}(\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}) \subset p\sigma(\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}).$$

Comme σ est injectif, on peut alors définir une application

$$\psi = \psi_{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}} : \mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \longrightarrow \mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$$

en posant pour tout $x \in \mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$:

$$\psi(x) = \frac{1}{p}\sigma^{-1}\big(\mathrm{Tr}_{\mathcal{E}^{\mathrm{nr}}/\sigma(\mathcal{E}^{\mathrm{nr}})}(x)\big).$$

C'est un homomorphisme de groupe, G_K-équivariant, qui vérifie, pour tout a et tout b dans $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$:

$$\psi(a\sigma(b)) = b\psi(a) \quad \text{et} \quad \psi(1) = 1.$$

Il induit une application

$$\psi = \psi_{\mathcal{O}_{\mathcal{E}(K)}} : \mathcal{O}_{\mathcal{E}(K)} \longrightarrow \mathcal{O}_{\mathcal{E}(K)}$$

commutant avec l'action de Γ_K, par restriction aux éléments fixes par G_{E_K}.

3.1.2. Cas général.

PROPOSITION 3.1. — *Soit M un Φ-Γ_K-module étale de torsion sur $\mathcal{O}_{\mathcal{E}(K)}$. Il existe une unique application additive*

$$\psi = \psi_M : M \longrightarrow M$$

vérifiant

$$\psi_M(a\phi_M(x)) = \psi_{\mathcal{O}_{\mathcal{E}(K)}}(a)x, \quad \forall a \in \mathcal{O}_{\mathcal{E}(K)},\ x \in M. \tag{1}$$

Cette application est surjective et vérifie $\psi_M \circ \phi_M = \mathrm{id}_M$ et

$$\psi_M\big(\sigma(a)x\big) = a\psi_M(x), \quad \forall a \in \mathcal{O}_{\mathcal{E}(K)},\ x \in M. \tag{2}$$

Preuve. — L'unicité résulte de ce que, comme M est étale, il est engendré, comme $\mathcal{O}_{\mathcal{E}(K)}$-module par l'image de ϕ_M.

On peut vérifier l'existence ainsi : l'équivalence de catégorie V_K (th. 1.2) associe à M une représentation de p-torsion V, qui nous permet d'identifier M à $D_K(V)$ et ϕ_M à la restriction de $\sigma \otimes \mathrm{id}_V$. Via $D_K \circ V_K$, on constate que l'application $\psi_M : M \to M$ induite par $\psi_{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}} \otimes \mathrm{id}_V$ convient. Le reste de la proposition est évident. □

3.2. Premières propriétés.

Dans toute la suite du § 3, n est un entier ≥ 1, M est un Φ-Γ_K-module étale sur $\mathcal{O}_{\mathcal{E}(K)}$, tué par p^n et $V = V_K(M)$.

On pose

$$\ell_V = \mathrm{long}_{\mathbb{Z}_p}(V).$$

Alors M est un $\mathcal{O}_{\mathcal{E}(K)}$-module de longueur ℓ_V ; c'est donc aussi un $\mathcal{O}_{\mathcal{E}_0}$-module de longueur $d_K\ \ell_V$; comme $\mathcal{O}_{\mathcal{E}_0}$ est la complétion p-adique de $W((\pi_0))$ et comme M est de p-torsion, M est encore un $W((\pi_0))$-module de longueur $d_K\ell_V$ (*cf.* 1.1.2).

PROPOSITION 3.2. — *On a les propriétés suivantes :*

1) *L'application ψ est continue.*

2) *Pour tout entier $r \geq 1$, $\mathrm{Ker}(\psi^r)$ est un sous-$\sigma^r(\mathcal{O}_{\mathcal{E}(K)})$-module de M de longueur finie égale à $(p^r - 1)\ell_V$ (donc aussi un $W((\sigma^r(\pi_0)))$-module de longueur $(p^r - 1)d_K\ell_V$), stable par Γ_K et :*

$$M = \mathrm{Ker}(\psi^r) \oplus \phi^r(M), \quad \mathrm{Ker}(\psi^r) = \bigoplus_{i=0}^{r-1} \phi^i(\mathrm{Ker}\,\psi).$$

De plus, l'application de $(\mathrm{Ker}\,\psi)^r$ dans $\mathrm{Ker}(\psi^r)$ qui à la famille $(a_i)_{0\leq i\leq r-1}$ associe $\sum_{i=0}^{r-1} \phi^i(a_i)$ est un isomorphisme de groupes Γ_K-équivariant.

3) *Pour tout* $x \in M$, $\psi(x)$ *est l'unique élément* y *de* M *tel que* $x - \phi(y) \in \operatorname{Ker}\psi$.

4) *L'application naturelle*

$$\operatorname{Ker}\psi \longrightarrow M/\phi(M)$$

est un homéomorphisme $\sigma(\mathcal{O}_{\mathcal{E}(K)})$*-linéaire et* Γ_K*-équivariant.*

5) *Si on note* M_{nil} *l'ensemble des éléments* ψ*-nilpotents de* M, *l'application de* $\bigoplus_{i\in\mathbb{N}} \operatorname{Ker}\psi$ *dans* M_{nil} *qui à la suite presque nulle* $(a_i)_{i\in\mathbb{N}}$ *associe* $\sum_{i\in\mathbb{N}} \phi^i(a_i)$ *est un isomorphisme de groupes qui commute avec l'action de* Γ_K.

Preuve. — L'assertion 1) est immédiate sur la définition de ψ. Montrons le 2). On déduit, par récurrence sur r du (2) de la proposition 3.1 que, pour tout entier $r \geq 1$, si $a \in \mathcal{O}_{\mathcal{E}(K)}$ et $x \in M$, alors $\psi^r(\sigma^r(a)x) = a\psi^r(x)$ et $\operatorname{Ker}(\psi^r)$ est bien un sous-$\sigma^r(\mathcal{O}_{\mathcal{E}(K)})$-module de M. Comme $\mathcal{O}_{\mathcal{E}(K)}$ est fini sur $\sigma^r(\mathcal{O}_{\mathcal{E}(K)})$, M est un $\sigma^r(\mathcal{O}_{\mathcal{E}(K)})$-module de longueur finie et $\operatorname{Ker}\psi^r$ aussi.

Pour tout $x \in M$, et tout entier naturel r, on a $x - \phi^r(\psi^r(x)) \in \operatorname{Ker}(\psi^r)$. Donc

$$M = \phi^r(M) + \operatorname{Ker}(\psi^r).$$

De plus, si $\phi^r(x)$ appartient à $\operatorname{Ker}(\psi^r)$, alors $x = \psi^r(\phi^r(x)) = 0$, donc $\phi^r(x) = 0$ et la somme est directe.

En particulier, tout x dans M s'écrit (de manière unique) sous la forme $x = \phi(y) + z$ avec y, z dans M et $\psi(z) = 0$, et on a donc $\psi^r(x) = \psi^{r-1}(y)$ pour tout $r \geq 1$. On en déduit alors par récurrence sur r que :

$$\forall r \geq 1, \quad \operatorname{Ker}(\psi^r) = \sum_{i=0}^{r-1} \phi^i(\operatorname{Ker}\psi).$$

Mais cette somme est directe : en effet, soit m un entier compris entre 0 et $(r-1)$; alors l'égalité $\sum_{i=0}^{r-1} \phi^i(x_i) = 0$ pour des éléments x_i dans $\operatorname{Ker}\psi$ entraîne, en appliquant ψ^m :

$$x_m = -\sum_{i=m+1}^{r-1} \phi^{i-m}(x_i) \quad \text{si} \quad m \leq r-2, \quad x_{r-1} = 0.$$

Dans tous les cas, $x_m \in \phi(M) \cap \operatorname{Ker}\psi$ et est donc nul ainsi que $\phi^m(x_m)$. On en déduit que pour tout entier $r \geq 1$, l'application de $(\operatorname{Ker}\psi)^r$ vers $\operatorname{Ker}(\psi^r)$ qui à $(x_i)_{0\leq i\leq r-1}$ associe $\sum_{i=0}^{r-1} \phi^i(x_i)$ est une bijection. Elle est de plus clairement additive.

Enfin, on a

$$\log_{\sigma^r(\mathcal{O}_{\mathcal{E}(K)})}(M) = p^r \log_{\mathcal{O}_{\mathcal{E}(K)}}(M),$$
$$\log_{\sigma^r(\mathcal{O}_{\mathcal{E}(K)})}\big(\phi^r(M)\big) = \log_{\mathcal{O}_{\mathcal{E}(K)}}(M).$$

Comme $M = \mathrm{Ker}(\psi^r) \oplus \phi^r(M)$, on obtient

$$\begin{aligned}\log_{\sigma^r(\mathcal{O}_{\mathcal{E}(K)})}(\mathrm{Ker}\,\psi) &= \log_{\sigma^r(\mathcal{O}_{\mathcal{E}(K)})}(M) - \log_{\sigma^r(\mathcal{O}_{\mathcal{E}(K)})}\big(\phi^r(M)\big)\\ &= (p^r - 1)\log_{\mathcal{O}_{\mathcal{E}(K)}}(M) = (p^r - 1)\,\ell_V.\end{aligned}$$

D'où le 2).

Les trois autres assertions s'en déduisent aisément. □

PROPOSITION 3.3. — *Le $W((\pi_0))$-module de type fini M contient un π_0-réseau $\mathcal{N}$ stable par ψ et Γ_K tel que :*

$$\psi(\mathcal{N}) = \mathcal{N} \quad et \quad M = \mathcal{N} + M_{\mathrm{nil}}.$$

Commençons par établir un lemme :

LEMME 3.4. — *Soit N un sous-$W[[\pi_0]]$-module de M. Alors :*

1) *$\psi(N)$ est un sous-$W[[\pi_0]]$-module de M.*

2) *Si N est de type fini sur $W[[\pi_0]]$, $\psi(N)$ l'est aussi.*

3) *Posons $q_n = \pi_0^{p^{n-1}}$. Si N est stable par ϕ, on a :*

$$\forall r \in \mathbb{N},\ \forall i \in \mathbb{Z}, \quad \psi^r(q_n^i N) \supset q_n^{\sup(0,i)} N.$$

Preuve.

1) Pour tout $x \in N$ et tout $\lambda \in W[[\pi_0]]$, on a $\lambda\psi(x) = \psi(\sigma(\lambda)x)$. Comme ψ est additive, $\psi(N)$ est bien un sous-$W[[\pi_0]]$-module de M.

2) Comme $W[[\pi_0]]$ est fini sur $W[[\sigma(\pi_0)]]$, si N est de type fini sur $W[[\pi_0]]$, il l'est aussi sur $W[[\sigma(\pi_0)]]$ donc $\psi(N)$ est de type fini sur $\sigma^{-1}(W[[\sigma(\pi_0)]]) = W[[\pi_0]]$.

3) Pour tout $x \in N$ et tout $r \in \mathbb{N}$, $\psi^r(\phi^r(x)) = x$, donc $\psi^r(N)$ contient N. Soit i un entier relatif :

• si i est négatif : $\psi^r(q_n^i N)$ contient $\psi^r(N)$ et donc N d'après ce qui précède ;

• si i est positif : comme $\sigma(\pi_0) \equiv \pi_0^p \bmod p$, $\phi(q_n) \equiv q_n^p (\mathrm{mod}\ p^n)$, donc $\phi(q_n^i x) = (q_n^i)^p\ \phi(x)$, pour tout $x \in N$. Donc $q_n^i N$ est stable par ϕ et $\psi^r(q_n^i N)$ contient $q_n^i N$. □

Ce lemme implique :

COROLLAIRE 3.5. — *Soit N un π_0-réseau de M stable par ϕ. Alors pour tout entier relatif i et tout entier naturel r, $\psi^r(q_n^i N)$ est un π_0-réseau de M.*

Preuve de la proposition 3.3. — On va procéder en deux étapes : on construit d'abord un π_0-réseau $\mathcal{N}_0$ stable par ψ et Γ_K et sur lequel ψ est surjective; puis on élargi $\mathcal{N}_0$ de sorte qu'il vérifie la seconde condition.

1) Par la proposition 2.4, on sait que M contient un π_0-réseau N stable par ϕ et Γ_K. Pour tout $r \in \mathbb{N}$, on a $\psi^r(N) \subset \psi^{r+1}(N)$ et le corollaire 3.5 nous montre alors que $(\psi^r(N))_{r\in\mathbb{N}}$ est une suite croissante de π_0-réseaux de M. On va prouver qu'elle est stationnaire et on pourra donc prendre pour $\mathcal{N}_0$ la limite de cette suite (qui sera bien stable par Γ_K puisque N l'est, et ψ et Γ_K commutent).

Rappelons qu'on a choisi $n \geq 1$ tel que p^n annule M. Toujours grâce au corollaire 3.5, $\psi(q_n^{-i}N)$ est un π_0-réseau pour tout entier i et il existe donc un entier s tel que $q_n^{-s}N$ contienne les π_0-réseaux $\psi(q_n^{-i}N)$ pour $i \in \{0, \ldots, p-1\}$. Considérons alors la suite d'entiers définie par :

$$s_1 = s, \quad s_{r+1} = s + t_r,$$

où t_r est la partie entière de s_r/p. On va prouver par récurrence que pour tout entier $r \geq 1$, $\psi^r(N)$ est contenu dans le π_0-réseau $q_n^{-s_r}N$: c'est clair pour $r = 1$; supposons alors que ce soit vrai pour un entier $r \geq 1$. Alors, par division euclidienne, $s_r = pt_r + i_r$, où i_r est un entier compris entre 0 et $(p-1)$, et $\psi^{r+1}(N)$ est contenu dans $\psi(q_n^{-s_r}N) = q_n^{-t_r}\psi(q_n^{-i_r}N)$, donc, par choix de s, dans $q_n^{-t_r-s}N = q_n^{-s_{r+1}}N$. Ce qui achève la récurrence.

Or la suite $(s_r)_{r\geq 1}$ est majorée par la partie entière de $sp/(p-1)$ que l'on notera ℓ. On en déduit que pout tout r, $\psi^r(N)$ est contenu dans le π_0-réseau $q_n^{-\ell}N$ qui est un $W[[\pi_0]]$-module noethérien, donc la suite croissante $\psi^r(N)$ est bien stationnaire.

2) Construisons maintenant $\mathcal{N}$. Donnons-nous un π_0-réseau $\mathcal{N}_0$ de M stable par ψ et Γ_K et tel que $\psi(\mathcal{N}_0) = \mathcal{N}_0$.

Le lemme 1.1 entraîne que pour tout $g \in \Gamma_k$, les éléments $q_n = \pi_0^{p^{n-1}}$ et $g(q_n)$ engendrent le même idéal de $W[[\pi_0]]$; par conséquent le π_0-réseau $q_n^{-1}\mathcal{N}_0$ est stable par Γ_K. Comme

$$\psi(q_n^{-1}\mathcal{N}_0) \subset \psi(q_n^{-p}\mathcal{N}_0) = q_n^{-1}\psi(\mathcal{N}_0) = q_n^{-1}\mathcal{N}_0,$$

il l'est aussi par ψ.

Par le corollaire 3.5, $(\psi^r(q_n^{-1}\mathcal{N}_0))_{r\in\mathbb{N}}$ est une suite décroissante de π_0-réseaux de M contenant tous $\mathcal{N}_0$ $(= \psi^r(\mathcal{N}_0)$ pour tout entier naturel $r)$. Cette suite est donc stationnaire et on note $\mathcal{N}$ sa limite. Il est clair que $\mathcal{N}$ est un π_0-réseau de M stable par ψ et Γ_K et que l'on a $\psi(\mathcal{N}) = \mathcal{N}$.

Enfin, soit $x \in M$. Choisissons un entier naturel r tel que $y = q_n^{p^r} x$ soit dans $\mathcal{N}_0$. L'élément $\psi^r(x)$ appartient alors à $q_n^{-1}\mathcal{N}_0$, et par construction de $\mathcal{N}$, il existe r' tel que $\psi^{r'}(x) \in \mathcal{N}$. Comme ψ est surjective sur $\mathcal{N}$, il existe $z \in \mathcal{N}$ tel que $\psi^{r'}(x) = \psi^{r'}(z)$. On a alors $x = z + (x - z)$ avec $z \in \mathcal{N}$ et $(x - z) \in M_{\mathrm{nil}}$. □

PROPOSITION 3.6. — *On a les propriétés suivantes :*

1) *Soit M' le plus grand sous-W-module de M contenu dans $(\psi-1)(M)$. Le W-module M/M' est de longueur finie.*

2) *Si K est une extension finie de $\mathbb{Q}_p$, le groupe $M/(\psi-1)(M)$ est fini.*

Preuve. — Soit $\mathcal{R}$ un π_0-réseau de M stable par ϕ sur lequel $\phi - 1$ est bijectif (*cf.* prop. 2.4). On a

$$(\psi - 1)(M) \supset (\psi - 1)\big(\phi(M)\big) = (\phi - 1)(M) \supset (\phi - 1)(\mathcal{R}) = \mathcal{R}.$$

Comme $\psi - 1$ est bijectif sur M_{nil}, on a aussi $(\psi - 1)(M) \supset M_{\mathrm{nil}}$; de ce fait,

$$(\psi - 1)(M) \supset \mathcal{R} + M_{\mathrm{nil}}$$

et, pour vérifier 1), il suffit de montrer que, si $M'' = \mathcal{R} + M_{\mathrm{nil}}$, alors le W-module M/M'' est de longueur finie.

Soit $\mathcal{N}$ comme dans la proposition 3.3. On voit que

$$M/M'' = (\mathcal{N} + M_{\mathrm{nil}})/(\mathcal{R} + M_{\mathrm{nil}})$$

s'identifie à un quotient de $\mathcal{N}/\mathcal{N} \cap \mathcal{R}$. Ce dernier W-module est de longueur finie comme quotient d'un π_0-réseau $\mathcal{N}$ de M par un autre π_0-réseau contenu dans $\mathcal{N}$.

Enfin, si $[K : \mathbb{Q}_p]$ est fini, k est fini, donc W est fini sur $\mathbb{Z}_p$ et tout W-module de longueur finie est un groupe fini. Donc M/M' et son quotient $M/(\psi - 1)(M)$ sont des groupes finis. □

3.3. Le théorème de structure.

3.3.1. Un résultat auxiliaire. — Posons

$$\pi_1 = \sigma(\pi_0).$$

Soit N un $W((\pi_1))$-module de longueur finie muni d'une action Γ_K-semi-linéaire et continue de Γ_K. La continuité de cette action implique que,

pour tout $x \in N$, la suite des $\tau^r(x)$ tend vers 0. Comme l'action de τ est W-linéaire, N a une structure naturelle de $W[[\tau]]$-module et tout sous-$W[[\pi_1]]$-module de N stable par Γ_K (en particulier tout π_1-réseau) est aussi un sous-$W[[\tau]]$-module.

PROPOSITION 3.7. — *Soit N un $W((\pi_1))$-module de longueur finie muni d'une action semi-linéaire et continue de Γ_K. On suppose que l'action de τ est inversible sur N, que N est aussi un $W((\tau))$-module de longueur finie et qu'il existe un π_1-réseau de N stable par Γ_K qui est aussi un τ-réseau. Alors :*

1) *Tout π_1-réseau de N stable par Γ_K est encore un τ-réseau.*

2) *Pour tout π_1-réseau S de N, il existe des π_1-réseaux S_1 et S_2 de N stable par Γ_K tels que $S_1 \subset S \subset S_2$.*

3) *Pour tout τ-réseau T de N, il existe des π_1-réseaux T_1 et T_2 de N stable par Γ_K tels que $T_1 \subset T \subset T_2$.*

Preuve.

1) Soient S_0 et S deux π_1-réseaux de N stables par Γ_K. Supposons que S_0 soit un τ-réseau et montrons que S en est aussi un :

a) Si $S_0 \subset S$, alors S contient un τ-réseau. En outre Γ_K opère linéairement sur le W-module de longueur finie S/S_0 ; on en déduit que τ^r opère trivialement sur ce quotient pour r assez grand donc que $\tau^r S \subset S_0$, ou encore que S est contenu dans le τ-réseau $\tau^{-r}S_0$. On en déduit que S est bien un τ-réseau.

b) Si $S \subset S_0$, alors S est contenu dans un τ-réseau. Comme Γ_K opère linéairement sur le W-module de longueur finie S_0/S, on voit que τ^s agit trivialement sur S_0/S pour s assez grand. Donc S, qui contient le τ-réseau $\tau^s S_0$, en est un aussi.

c) Dans le cas général, $S_0 + S$ est un τ-réseau grâce à (a), et (b) montre donc que S aussi.

2) Si S_0 est comme ci-dessus et si S est un π_1-réseau de N, il existe des entiers $r, s \in \mathbb{Z}$ tels que $\pi_1^s S_0 \subset S \subset \pi_1^r S_0$ et l'assertion résulte de ce que, comme l'idéal de $W[[\pi_1]]$ engendré par π_1 est stable par Γ_K (*cf.* lemme 1.1), les π_1-réseaux $\pi_1^s S_0$ et $\pi_1^r S_0$ le sont aussi.

3) Remarquons d'abord que, pour tout $i \in \mathbb{N}$, il existe $r \in \mathbb{N}$ tel que $\pi_1^r S_0 \subset \tau^i S_0$: en effet la suite des $\pi_1^r S_0 + \tau^i S_0$, pour $r \in \mathbb{N}$, est une suite décroissante de sous-W-modules de S_0 contenant $\tau^i S_0$. Comme $S_0/\tau^i S_0$ est un W-module de longueur finie, il existe r tel que $\pi_1^r S_0 + \tau^i S_0 = \pi_1^{r+1} S_0 + \tau^i S_0$ et, comme S_0 est séparé et complet pour la topologie π_1-adique, on en déduit que $\pi_1^r S_0 \subset \tau^i S_0$.

De même, pour tout $j \in \mathbb{N}$, il existe $s \in \mathbb{N}$ tel que $\tau^{-j}S_0 \subset \pi_1^{-s}S_0$: en effet, comme N est la réunion des $\pi_1^{-s}S_0$, la suite des $\tau^{-j}S_0 \cap \pi_1^{-s}S_0$, pour $s \in \mathbb{N}$, est une suite croissante de sous-W-modules de $\tau^{-j}S_0$ dont la réunion est $\tau^{-j}S_0$. Comme les éléments de cette suite contiennent S_0 et comme $\tau^{-j}S_0/S_0$ est un-W-module de longueur finie, il existe $s \in \mathbb{N}$ tel que $\pi_1^{-s}S_0 \cap \tau^{-j}S_0 = \tau^{-j}S_0$ et $\tau^{-j}S_0 \subset \pi_1^{-s}S_0$.

Si T est alors un τ-réseau de N et si S_0 est comme plus haut, il existe des entiers $i, j \in \mathbb{N}$ tels que $\tau^i S_0 \subset T \subset \tau^{-j}S_0$ et il suffit de prendre $T_1 = \pi_1^r S_0$ et $T_2 = \pi_1^{-s}S_0$ où r et s sont comme ci-dessus. □

3.3.2. Énoncé du théorème. — Rappelons (prop. 3.2) que $\operatorname{Ker}\psi$ est un $W((\pi_1))$-module de longueur finie égale à $(p-1)\,\ell_V$. Soit $\mathcal{R}'$ un π_0-réseau de M stable par ϕ et Γ_K (un tel réseau existe d'après la prop. 2.4). Pour tout $x \in M$, on a

$$x = \phi\big(\psi(x)\big) + \big(x - \phi(\psi(x))\big)\,;$$

donc, dans la décomposition en somme directe $M = \phi(M) \oplus \operatorname{Ker}\psi$, on voit que

$$\mathcal{R}' = \phi(\mathcal{R}') \oplus (\mathcal{R}' \cap \operatorname{Ker}\psi)$$

et que $\mathcal{R}' \cap \operatorname{Ker}\psi$ est un π_1-réseau de $\operatorname{Ker}\psi$ stable par Γ_K.

THÉORÈME 3.8. — *Le noyau de ψ a la structure suivante* :

1) *Soit e_K l'indice de ramification absolu de K. L'action de τ est bijective sur* $\operatorname{Ker}\psi$, *qui est un $W((\tau))$-module de longueur finie, égale à* $e_K\ell_V = e_K \operatorname{long}_{\mathcal{O}_{\mathcal{E}(K)}}(M)$.

2) *Tout π_1-réseau de* $\operatorname{Ker}\psi$ *stable par Γ_K est aussi un τ-réseau.*

Remarquons que, comme la topologie de $\operatorname{Ker}\psi$ induite par celle de M est sa topologie de $W((\pi_1))$-module de longueur finie, ce théorème, compte tenu de la proposition précédente, implique que *cette topologie coincide avec sa topologie de $W((\tau))$-module de longueur finie.*

Nous allons d'abord énoncer un lemme, puis en déduire le théorème.

3.3.3. Le lemme fondamental. — Remarquons que si F est un corps valué complet à corps résiduel de caractéristique p, le groupe U_F des unités fondamentales de F est, de façon naturelle, un $\mathbb{Z}_p$-module.

LEMME 3.9. — *Supposons l'extension K_∞/K totalement ramifiée, soient π une uniformisante de E_K, $\omega = \gamma(\pi)/\pi$ et $\alpha \in \mathbb{Z}_p$. Rappelons que ω appartient à U_{E_K} (cf. lemme* 1.1).

1) *Il existe sur E_K une et une seule action $k[[\tau]]$-linéaire continue*

$$(\lambda, x) \longmapsto \lambda * x \quad \text{pour} \quad \lambda \in k[[\tau]],\ x \in E_K,$$

telle que, pour tout $x \in E_K$, $\lambda * x = \lambda x$ si $\lambda \in k$ et $\gamma * x = \omega^{\alpha}\gamma(x)$.

On suppose que p divise α.

2) *Alors $\sigma(E_K)$ est un sous-$k[[\tau]]$-module de E_K et τ est inversible sur $E_K/\sigma(E_K)$, qui devient ainsi un $k((\tau))$-espace vectoriel de dimension finie égale à e_K.*

3) *Sur ce quotient, l'image S_α de $\mathcal{O}_{E_K}$ est aussi bien un τ-réseau qu'un π_1-réseau.*

La démonstration de ce lemme constitue le cœur technique de cet article et est l'objet du § 5. Dans la suite, on écrit $E_{K,\alpha}$ pour E_K muni de la structure de $k[[\tau]]$-module ainsi définie et, si p divise α, on note $\sigma(E_K)_\alpha$ le sous-module considéré et $\widetilde{E}_{K,\alpha}$ le quotient $E_{K,\alpha}/\sigma(E_K)_\alpha$.

3.3.4. Preuve du théorème. — Rappelons que n désigne un entier tel que p^n annule V (et donc aussi M) ; pour tout anneau A, on note $W_n(A)$ l'anneau des vecteurs de Witt de longueur n à coefficients dans A.

1) *Remplacement de K par une extension finie galoisienne non ramifiée.* Soit K' une extension finie galoisienne non ramifiée de K contenue dans $\overline{K}$; par restriction $G_{K'} = \mathrm{Gal}(\overline{K}/K')$ opère aussi sur V. Rappelons que M s'identifie à $D_K(V) = (\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \otimes_{\mathbb{Z}_p} V)^{G_K}$; si $M' = D_{K'}(V)$, alors M' s'identifie à $(\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \otimes_{\mathbb{Z}_p} V)^{G_{K'}}$ et aussi à $\mathcal{O}_{\mathcal{E}}(K') \otimes_{\mathcal{O}_{\mathcal{E}(K)}} M$.

Avec des notations évidentes, on voit que

$$\mathcal{O}_{\mathcal{E}(K)} = \mathcal{O}_{\mathcal{E}(K' \cap K_\infty)}$$

tandis que

$$\mathcal{O}_{\mathcal{E}(K')} = W(k') \otimes_{W(k' \cap k_\infty)} \mathcal{O}_{\mathcal{E}(K' \cap K_\infty)},$$

ce qui fait que $M' = W_n(k') \otimes_{W_n(k' \cap k_\infty)} M$, donc aussi que

$$\mathrm{Ker}\, \psi_{M'} = W_n(k') \otimes_{W_n(k' \cap k_\infty)} \mathrm{Ker}\, \psi_M.$$

De plus, $M = (M')^{\mathrm{Gal}(K'/K' \cap K_\infty)}$ et

$$\mathrm{Ker}\, \psi_M = (\mathrm{Ker}\, \psi_{M'})^{\mathrm{Gal}(K'/K' \cap K_\infty)}.$$

Supposons le théorème vrai pour M'. Soient

$$a = (\Gamma_K : \Gamma_{K'}), \quad \gamma' = \gamma^a, \quad \tau' = \gamma' - 1.$$

Alors τ' est bijectif sur $\operatorname{Ker}\psi_{M'}$ qui est un $W_n(k')((\tau'))$-module de longueur finie égale à $e_{K'}\,\ell_V = e_K\,\ell_V$; on voit aussi que τ', et *a fortiori* τ, est bijectif sur $\operatorname{Ker}\psi_M$ et que

$$\operatorname{Ker}\psi_{M'} = W_n(k')\big((\tau')\big) \otimes_{W_N(k'\cap k_\infty)((\tau'))} \operatorname{Ker}\psi_M\ ;$$

en particulier, $\operatorname{Ker}\psi_M$ est un $W_n(k'\cap k_\infty)((\tau'))$-module de longueur finie égale à $e_K\ell_V$.

Par ailleurs, $W_n(k)((\tau))$ est libre de rang a sur $W_n(k)((\tau'))$, donc

$$\operatorname{long}_{W_n(k)((\tau'))}(\operatorname{Ker}\psi_M) = a\operatorname{long}_{W_n(k)((\tau))}(\operatorname{Ker}\psi_M).$$

On a aussi

$$a = [K'\cap K_\infty : K] = [k'\cap k_\infty : k]$$

et $W_n(k'\cap k_\infty)((\tau'))$ est libre de rang a sur $W_n(k)((\tau'))$, donc

$$\operatorname{long}_{W_n(k)((\tau'))}(\operatorname{Ker}\psi_M) = a\operatorname{long}_{W_n(k'\cap k_\infty)((\tau'))}(\operatorname{Ker}\psi_M),$$

ce qui fait que

$$\operatorname{long}_{W_n(k)((\tau))}(\operatorname{Ker}\psi_M) = \operatorname{long}_{W_n(k'\cap k\infty)((\tau'))}(\operatorname{Ker}\psi_M) = e_K\ell_V,$$

d'où l'assertion 1) du théorème pour M.

Enfin, soient S un π_1-réseau stable par Γ_K du $W(k)((\pi_1))$-module $\operatorname{Ker}\psi_M$ et soit S_1 le sous-$W(k'\cap k_\infty)$-module de $\operatorname{Ker}\psi_M$ engendré par S. Alors S_1 est encore un π_1-réseau de $\operatorname{Ker}\psi_M$ stable par Γ_K et, d'après la proposition 3.7, il suffit de vérifier que S_1 est bien un τ-réseau. Mais

$$S' = W(k') \otimes_{W(k'\cap k_\infty)} S_1$$

est un π_1-réseau de $\operatorname{Ker}\psi_{M'}$ (vu comme $W(k')((\pi_1))$-module de type fini) stable par Γ_K, donc *a fortiori* par $\Gamma_{K'}$.

Si l'on admet le théorème pour M', il en résulte que S' est un τ'-réseau du $W(k')((\tau'))$-module $\operatorname{Ker}\psi_{M'}$. Comme S_1 s'identifie à $(S')^{\operatorname{Gal}(K'/K'\cap K_\infty)}$, on en déduit que S_1 est un τ'-réseau du $W(k'\cap k_\infty)((\tau'))$-module $\operatorname{Ker}\psi_M$. Puisque S_1 est stable par τ, c'est alors un τ-réseau de $\operatorname{Ker}\psi_M$, vu comme $W(k)((\tau))$-module.

On peut donc, pour prouver le théorème remplacer K par K'.

2) *Réduction au cas où M est simple.* On s'y ramène par récurrence sur la longueur de M. En effet, soit

$$0 \to M' \longrightarrow M \longrightarrow M'' \to 0$$

une suite exacte de Φ-Γ_K-modules étales sur $\mathcal{O}_{\mathcal{E}(K)}$. Comme l'action de ψ est surjective sur M', elle induit une suite exacte

$$0 \to \operatorname{Ker}\psi_{M'} \longrightarrow \operatorname{Ker}\psi_M \longrightarrow \operatorname{Ker}\psi_{M''} \to 0.$$

La bijectivité de τ sur $\operatorname{Ker}\psi_M$ se déduit de la bijectivité de τ sur $\operatorname{Ker}\psi_{M'}$ et $\operatorname{Ker}\psi_{M''}$, de même que l'assertion sur la longueur de $\operatorname{Ker}\psi_M$ résulte des assertions analogues pour $\operatorname{Ker}\psi_{M'}$ et $\operatorname{Ker}\psi_{M''}$.

Si S est un π_1-réseau de $\operatorname{Ker}\psi_M$ stable par Γ_K, son image S'' dans $\operatorname{Ker}\psi_{M''}$ est un π_1-réseau de $\operatorname{Ker}\psi_{M''}$ stable par Γ_K, tandis que le noyau S' de la projection de S sur S" est un π_1-réseau de $\operatorname{Ker}\psi_{M'}$ stable par Γ_K. Le fait que S soit un τ-réseau de $\operatorname{Ker}\psi_M$ résulte alors de ce que S' est un τ-réseau de $\operatorname{Ker}\psi_{M'}$ et S'' un τ-réseau de $\operatorname{Ker}\psi_{M''}$.

3) *Fin de la preuve.* Soient G_V le noyau de l'action de G_K sur V, $L = \overline{K}^{G_V}$ et $J = \operatorname{Gal}(L/K)$. Grâce à 1) on peut supposer les extensions K_∞/K et L/K totalement ramifiées. Le fait que L/K le soit implique (*cf.* [Se1, cor. 4, p. 75]) que J est le produit semi-direct d'un p-groupe invariant P par un groupe cyclique J' dont l'ordre m est premier à p. Grâce à 2), on peut supposer que V est simple; ceci entraîne que V est tuée par p et aussi que P est trivial (car V^P est un sous-$\mathbb{F}_p[J]$-module de V non trivial : *cf.* [Se1, th. 2, p. 146]), donc que $J = J'$.

Soit $E_L = (E^{\mathrm{sep}})^{G_V \cap \operatorname{Gal}(\overline{K}/K_\infty)}$. Le groupe de Galois (respectivement le groupe d'inertie) de l'extension E_L/E_K s'identifie à l'image du groupe $\operatorname{Gal}(\overline{K}/K_\infty)$ (respectivement du sous-groupe d'inertie de $\operatorname{Gal}(\overline{K}/K_\infty)$) dans J. Comme J est d'ordre premier à p, cette image est J et E_L/E_K est une extension totalement ramifiée, cyclique d'ordre m. Si q est la plus petite puissance de p telle que m divise $q-1$, ceci entraîne (*cf.* [Se1, cor. 1, p. 75]) que le corps résiduel k de E_K contient un corps à q éléments, que nous notons F_0, qu'il existe une uniformisante π_L de E_L telle que $\pi = \pi_L^m$ est une uniformisante de E_K et que le caractère

$$\eta_0 : J \longrightarrow F_0^*,$$

défini par $\eta_0(g) = g(\pi_L)/\pi_L$, engendre le groupe dual de J.

Par ailleurs, si $V^* = \operatorname{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p)$ désigne la représentation duale, on voit que V^* est de dimension 1 sur le corps

$$F = \operatorname{End}_{\mathbb{F}_p[\operatorname{Gal}(\overline{K}/K_\infty)]}(V) = \operatorname{End}_{\mathbb{F}_p[J]}(V),$$

qui est aussi un corps à q éléments. On choisit un générateur de V^* sur F, ce qui nous permet d'identifier V^* à F muni de l'action de J donnée par un caractère $\eta : J \to F^*$: pour $g \in J$ et $v^* \in V^*$, on a donc $g(v^*) = \eta(g)v^*$.

La projection de M sur $M/\phi(M)$ induit un isomorphisme, compatible avec toutes les structures, de $\operatorname{Ker}\psi$ sur $M/\phi(M)$, ce qui nous permet, pour prouver le théorème, de remplacer $\operatorname{Ker}\psi$ par $M/\phi(M)$.

Si $G = \operatorname{Gal}(\overline{K}/K_\infty)$, on a

$$\begin{aligned} M &= (\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \otimes_{\mathbb{Z}_p} V)^G &&= (E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} V)^G \\ &= \operatorname{Hom}_{\mathbb{F}_p[G]}(V^*, E^{\mathrm{sep}}) &&= \operatorname{Hom}_{\mathbb{F}_p[J]}(V^*, E_L) \end{aligned}$$

et c'est un E_K-espace vectoriel de dimension $\ell_V = \dim_{\mathbb{F}_p}(V) = [F : \mathbb{F}_p]$.

L'ensemble T des $\mathbb{F}_p$-plongements de F dans F_0 a $\dim_{\mathbb{F}_p}(V^*) = \ell_V$ éléments. Pour chaque $t \in T$, notons a_t l'unique entier vérifiant $0 \leq a_t < m$ tel que $t \circ \eta = \eta_0^{a_t}$. Notons

$$e_t : V^* \longrightarrow E_L$$

l'application définie par

$$e_t(v^*) = t(v^*)\ \pi_L^{a_t}.$$

Pour tout $g \in J$ et tout $v^* \in V^*$, on a alors :

$$e_t\big(g(v^*)\big) = t\big(\eta(g)v^*\big)\pi_L^{a_t} = \eta_0^{a_t}(g)t(v^*)\pi_L^{a_t} = g\big(t(v^*)\big)\pi_L^{a_t} = g\big(e_t(v^*)\big).$$

Les e_t sont donc dans M et ils sont linéairement indépendants sur E_K ; de ce fait, ils forment une base de M sur E_K. Si $e'_t = \phi(e_t) = \sigma \circ e_t$, il en est de même des e'_t. Les applications

$$\theta : (E_K)^T \longrightarrow M, \quad \theta' : (E_K)^T \longrightarrow M$$

définies par

$$\theta((x_t)_{t\in T}) = \sum_{t\in T} x_t e_t, \quad \theta((y_t)_{t\in T}) = \sum_{t\in T} y_t e'_t$$

sont donc des isomorphismes de E_K-espaces vectoriels.

L'action de Γ_K sur E_K s'étend de manière unique à E_L : si $\gamma(\pi) = \omega\pi$, on a $\gamma(\pi_L) = \omega^{1/m}\pi_L$. Pour tout $t \in T$, $e'_t(v) = t(v^p)\ \pi_L^{pa_t}$ et on en déduit que, si $\alpha_t = pa_t/m$, on a $\gamma(e'_t) = \omega^{\alpha_t}\ e'_t$. Par conséquent, l'application θ' peut aussi être considérée comme un isomorphisme de $k[[\tau]]$-modules

$$\theta' : \bigoplus_{t\in T} E_{K,\alpha_t} \longrightarrow M.$$

Si l'on écrit un élément $x \in M$ sous la forme $x = \sum_{t\in T} x_t\ e_t$, avec les $x_t \in E_K$, on voit que $\phi(x) = \sum_{t\in T} x_t^p e'_t$. On obtient ainsi, par passage

aux quotients à partir de l'inverse de θ' une bijection

$$\nu : M/\phi(M) \longrightarrow \bigoplus_{t\in T} \widetilde{E}_{K,\alpha_t},$$

qui est aussi bien un isomorphisme de $\sigma(E_K)$-espaces vectoriels que de $k[[\tau]]$-modules.

La première partie du théorème résulte alors de la deuxième assertion du lemme 3.9. D'après la proposition 3.7, il suffit de vérifier la deuxième partie pour un π_1-réseau S de $M/\phi(M)$ stable par Γ_K particulier. Si, avec les notations du lemme 3.9, on prend pour S l'image inverse par ν de $\bigoplus_{t\in T} S_{\alpha_t}$, la troisième assertion du lemme permet de conclure. □

3.4. Le cœur de M.

DÉFINITION 3.10. — *Si N est un $W((X))$-module de longueur finie, on appelle X-*pseudo-réseau *de N tout sous-groupe Λ de N stable par X qui contient un X-réseau Λ_1 et est contenu dans un X-réseau Λ_2 de N.*

Autrement dit, un X-pseudo-réseau est un sous-groupe ouvert stable par X qui est contenu dans un X-réseau.

Si k est fini, N est un $\mathbb{Z}_p((X))$-module de longueur finie égale à $[k : \mathbb{F}_p] \log_{W((X))}(N)$. Un X-pseudo-réseau n'est alors rien d'autre qu'un X-réseau de N, *considéré comme $\mathbb{Z}_p((X))$-module.*

On appelle *cœur de M* le sous-$\mathbb{Z}_p[[\tau]]$-module de M :

$$c(M) = (\phi - 1)M \cap \operatorname{Ker}\psi.$$

Si $x \in M$, alors $(\phi - 1)(x) \in \operatorname{Ker}\psi$ si et seulement si $\psi(x) = x$ de sorte que $c(M) = (\phi - 1)(M_{\psi=1})$.

PROPOSITION 3.10. — *Le cœur de M est un τ-pseudo-réseau de* $\operatorname{Ker}\psi$.

Preuve. — On sait (prop. 2.4) que M contient un π_0-réseau $\mathcal{R}$ sur lequel $\rho = \phi - 1$ est bijective; donc le groupe $(\phi - 1)M$ contient le π_0-réseau $\mathcal{R}$ et est ouvert dans M. Par conséquent $(\phi-1)M\cap\operatorname{Ker}\psi = c(M)$ est ouvert dans $\operatorname{Ker}\psi$.

Soit $\mathcal{N}$ comme dans la proposition 3.3. On a $M_{\psi=1} \subset \mathcal{N}$ et de ce fait :

$$c(M) = (\phi - 1)(M_{\psi=1}) \subset (\phi - 1)(\mathcal{N}) \cap \operatorname{Ker}\psi \subset (\mathcal{N} + \phi(\mathcal{N})) \cap \operatorname{Ker}\psi.$$

Mais $\mathcal{N}$ est un sous-$W[[\pi_0]]$-module de type fini de M, donc $\phi(\mathcal{N})$ est un sous-$W[[\pi_1]]$-module de type fini de M; comme $W[[\pi_0]]$ est fini sur

$W[[\pi_1]]$, on voit que $\mathcal{N}$ est aussi un sous-$W[[\pi_1]]$-module de type fini de M ; il en est donc de même de $\mathcal{N}+\phi(\mathcal{N})$. Finalement, $(\mathcal{N}+\phi(\mathcal{N}))\cap\operatorname{Ker}\psi$ est contenu dans un sous-$W[[\pi_1]]$-module de type fini de $\operatorname{Ker}\psi$, donc dans un π_1-réseau de $\operatorname{Ker}\psi$. L'assertion résulte alors de ce que, compte tenu de la proposition 3.7, le théorème 3.8 implique que tout π_1-réseau de $\operatorname{Ker}\psi$ est contenu dans un τ-réseau. □

COROLLAIRE 3.11. — *Si $[K:\mathbb{Q}_p]$ est fini, $c(M)/\tau(c(M))$ est un groupe fini d'ordre $p^{[K:\mathbb{Q}_p]\ell_V}$.*

Comme $\operatorname{Ker}\psi$ est un $\mathbb{Z}_p((\tau))$-module de longueur

$$[k:\mathbb{F}_p]\operatorname{long}_{W((\tau))}(\operatorname{Ker}\psi)=[k:\mathbb{F}_p]e_K\ell_V=[K:\mathbb{Q}_p]\ell_V,$$

ce corollaire résulte du lemme suivant :

LEMME 3.12. — *Si A est un $\mathbb{Z}_p((X))$-module de type fini tué par une puissance de p et B un X-réseau de A, alors B/XB est un groupe fini d'ordre p^ℓ, où ℓ est la longueur de A sur $\mathbb{Z}_p((X))$.*

Preuve. — Remarquons que $pA\cap B$ et $B/(pA\cap B)$ sont des X-réseaux de pA et A/pA respectivement. De plus, comme A est sans X-torsion, le lemme du serpent donne la suite exacte :

$$0\to\frac{pA\cap B}{X(pA\cap B)}\longrightarrow\frac{B}{XB}\longrightarrow\frac{B/(pA\cap B)}{X(B/(pA\cap B))}\to 0.$$

Par récurrence sur la plus petite puissance de p qui annule A, on peut donc supposer que $pA=0$. Dans ce cas, A est un $\mathbb{F}_p((X))$-espace vectoriel de dimension finie ℓ et B est un sous-$\mathbb{F}_p[[X]]$-module libre de rang ℓ. Donc B/XB est un $\mathbb{F}_p$-espace vectoriel de dimension ℓ, *i.e.* un groupe fini d'ordre p^ℓ. □

4. Calcul de la cohomologie galoisienne

Rappelons que n est un entier ≥ 1, M un Φ-Γ_K-module étale sur $\mathcal{O}_{\mathcal{E}(K)}$ tué par p^n, $V=V_K(M)$ et $\ell_V=\operatorname{long}_{\mathbb{Z}_p}(V)$.

Dans ce paragraphe, on adopte la convention suivante : dans tout complexe considéré, le premier terme écrit est placé en degré -1.

4.1. Un complexe filtré quasi-isomorphe à $C_{\phi,\gamma}(M)$.

Rappelons que la cohomologie galoisienne de V est la cohomologie du complexe $C_{\phi,\gamma}(M)$. On va commencer par montrer que cette cohomologie peut aussi se calculer en remplaçant ϕ par ψ dans les flèches de ce complexe. De façon précise :

PROPOSITION 4.1. — *Soit $C_{\psi,\gamma}(M)$ le complexe*

$$0 \longrightarrow M \longrightarrow M \oplus M \longrightarrow M \longrightarrow 0 \longrightarrow 0 \to \cdots,$$
$$x \longmapsto ((\psi - 1)(x), \tau(x)),$$
$$(y, z) \longmapsto \tau(y) - (\psi - 1)(z).$$

Soit $f : M \oplus M \to M \oplus M$ définie par $(y, z) \mapsto (-\psi(y), z)$. Alors, le morphisme de complexes

$$\begin{array}{lccccccccc} C_{\phi,\gamma}(M): & 0 & \longrightarrow & M & \longrightarrow & M \oplus M & \longrightarrow & M & \longrightarrow & 0 \to \cdots \\ & \downarrow 0 & & \downarrow \mathrm{id} & & \downarrow f & & \downarrow -\psi & & \downarrow 0 \\ C_{\psi,\gamma}(M): & 0 & \longrightarrow & M & \longrightarrow & M \oplus M & \longrightarrow & M & \longrightarrow & 0 \to \cdots \end{array}$$

est un quasi-isomorphisme.

Preuve. — Comme ψ est surjective, on voit que $C_{\psi,\gamma}(M)$ est le quotient, *via* le morphisme de complexes précédent, de $C_{\phi,\gamma}(M)$ par le sous-complexe :

$$0 \to 0 \longrightarrow \operatorname{Ker}\psi \oplus 0 \longrightarrow \operatorname{Ker}\psi \to 0 \to \cdots.$$

et la bijectivité de τ sur $\operatorname{Ker}\psi$ signifie que ce sous-complexe est acyclique. □

4.2. La filtration canonique de $C_{\psi,\gamma}(M)$.

Pour étudier la cohomologie du complexe $C(M) = C_{\psi,\gamma}(M)$, on va le munir d'une filtration en trois crans par des sous-complexes

$$C_{\psi,\gamma}(M) = C^0(M) \supset C^1(M) \supset C^2(M) \supset C^3(M)$$

en posant

$$C^1(M) : 0 \to M_{\psi=1} \xrightarrow{\tau} M_{\psi=1} \longrightarrow 0 \longrightarrow 0 \to \cdots,$$

$$C^2(M) : 0 \to M_{\phi=1} \xrightarrow{\tau} M_{\phi=1} \longrightarrow 0 \longrightarrow 0 \to \cdots,$$

et $C^3(M)$ est le complexe nul.

Pour $i \in \{0, 1, 2\}$, on définit

$$\operatorname{gr}^i C(M) = C^i(M)/C^{i+1}(M).$$

Remarquons que, comme $M_{\phi=1}$ s'identifie à $V^{\mathrm{Gal}(\overline{K}/K_\infty)}$, le complexe $\operatorname{gr}^2 C(M) = C^2(M)$ s'identifie au complexe

$$0 \to V^{\mathrm{Gal}(\overline{K}/K_\infty)} \xrightarrow{\tau} V^{\mathrm{Gal}(\overline{K}/K_\infty)} \longrightarrow 0 \longrightarrow 0 \to \cdots.$$

Le complexe $\operatorname{gr}^1 C(M)$ est

$$0 \to M_{\psi=1}/M_{\phi=1} \xrightarrow{\tau} M_{\psi=1}/M_{\phi=1} \longrightarrow 0 \longrightarrow 0 \to \cdots.$$

Pour $i = 0$, on a la description suivante :

LEMME 4.2. — *Le complexe* $\mathrm{gr}^0\,\mathcal{C}(M)$ *est quasi-isomorphe à* :

$$0 \to 0 \longrightarrow \frac{M}{(\psi-1)(M)} \xrightarrow{\tau} \frac{M}{(\psi-1)(M)} \longrightarrow 0 \to \cdots.$$

Preuve. — il suffit de montrer que le sous-complexe suivant de $\mathrm{gr}^0\,\mathcal{C}(M)$:

$$0 \to \frac{M}{M_{\psi=1}} \longrightarrow (\psi-1)(M) \oplus \frac{M}{M_{\psi=1}} \longrightarrow (\psi-1)(M) \to 0 \to \cdots$$

est acyclique, ce qui résulte imédiatement de ce que $\psi - 1$ induit une bijection de $M/M_{\psi=1}$ sur $(\psi-1)(M)$. □

4.3. La filtration associée sur la cohomologie.

L'anneau $\mathbb{Z}_p[[\Gamma_K]]$ s'identifie à l'anneau $\mathbb{Z}_p[[\tau]]$ des séries formelles en τ à coefficients dans $\mathbb{Z}_p$. Pour tout $\mathbb{Z}_p[[\Gamma_K]]$-module topologique N, on note $(H^i(\Gamma_K, N))_{i\in\mathbb{Z}}$ les groupes de cohomologie du complexe

$$0 \to N \xrightarrow{\tau} N \longrightarrow 0 \longrightarrow 0 \to \cdots$$

Lorsque N est un Γ_K-module discret, on voit facilement que ces groupes s'identifient aux groupes de cohomologie habituels.

On a défini une filtration en trois crans du complexe $\mathcal{C}_{\psi,\gamma}(M)$; la suite exacte longue de cohomologie associée à une suite exacte courte de complexes donne alors une filtration en trois crans des groupes de cohomologie $\mathcal{H}^i(M)$:

THÉORÈME 4.3. — *Pour tout entier naturel* i, *on a* :

- $H^i(\mathrm{gr}^0\,\mathcal{C}(M)) = H^{i-1}(\Gamma_K, M/(\psi-1)(M))$,
- $H^i(\mathrm{gr}^1\,\mathcal{C}(M)) = \{0\}$ *sauf si* $i = 1$ *et* $H^1(\mathrm{gr}^1\,\mathcal{C}(M)) = c(M)/\tau(c(M))$,
- $H^i(\mathrm{gr}^2\,\mathcal{C}(M)) = H^i(\Gamma_K, M_{\phi=1}) = H^i(\Gamma_K, V^{\mathrm{Gal}(\overline{K}/K_\infty)})$

ainsi que la filtration suivante :

$$\mathcal{H}^i(M) \supset H^i(\Gamma_K, M_{\psi=1}) \supset H^i(\Gamma_K, M_{\phi=1}),$$

avec

$$\frac{\mathcal{H}^i(M)}{H^i(\Gamma_K, M_{\psi=1})} \simeq H^i(\mathrm{gr}^0\,\mathcal{C}(M)) \quad \text{et} \quad \frac{H^i(\Gamma_K, M_{\psi=1})}{H^i(\Gamma_K, M_{\phi=1})} \simeq H^i(\mathrm{gr}^1\,\mathcal{C}(M)).$$

Preuve. — Les assertions concernant $\mathrm{gr}^0\,\mathcal{C}(M)$ et $\mathrm{gr}^2\,\mathcal{C}(M)$ sont évidentes. Pour $\mathrm{gr}^1\,\mathcal{C}(M)$, on remarque que $\phi-1$ induit un isomorphisme Γ_K-équivariant de $M_{\psi=1}/M_{\phi=1}$ sur $(\phi-1)(M_{\psi=1}) = (\phi-1)M \cap \mathrm{Ker}\,\psi = c(M)$. L'injectivité de l'action de τ sur $\mathrm{Ker}\,\psi$ permet de conclure. Le reste découle alors immédiatement de l'examen de suites exactes longues de cohomologie et de la nullité de certains groupes. □

4.4. Preuve du théorème B.

Compte-tenu des résultats du § 3, le théorème B se déduit immédiatement du théorème 4.3. En effet, $V^{\mathrm{Gal}(\overline{K}/K_\infty)}$ est un groupe fini et les $H^i(\mathrm{gr}^2\,\mathcal{C}(M))$ sont triviaux sauf peut-être H^0 et H^1 qui sont finis du même ordre. Si l'extension $K/\mathbb{Q}_p$ est finie, comme $M/(\psi-1)(M)$ est un groupe fini (proposition 3.6), les $H^i(\mathrm{gr}^0\,\mathcal{C}(M))$ sont triviaux sauf peut-être H^1 et H^2 qui sont finis du même ordre; enfin, les $H^i(\mathrm{gr}^1\,\mathcal{C}(M))$ sont triviaux sauf peut-être H^1 qui est un groupe fini d'ordre $p^{[K:\mathbb{Q}_p]\ell_V}$ (cor. 3.11). □

5. Preuve du lemme fondamental

L'objet essentiel de ce paragraphe est d'établir le lemme 3.9. On va en fait démontrer un résultat un peu plus général, à savoir le même énoncé en remplaçant K_∞ par une $\mathbb{Z}_p$-extension totalement ramifiée arbitraire de K. De façon précise :

THÉORÈME 5.1. — *Soit K_∞ une $\mathbb{Z}_p$-extension totalement ramifiée de K. Soient $\Gamma=\mathrm{Gal}(K_\infty/K)$, γ un générateur topologique de Γ et $\tau=\gamma-1$. Soient E le corps des normes de l'extension K_∞/K, π une uniformisante de E, $\omega=\gamma(\pi)/\pi$ et $\alpha\in\mathbb{Z}_p$. L'élément ω est une unité fondamentale de E.*

1) *Il existe sur E une et une seule action $k[[\tau]]$-linéaire continue*

$$(\lambda,x)\longmapsto \lambda * x \quad \text{pour} \quad \lambda\in k[[\tau]],\ x\in E,$$

telle que, pour tout $x\in E$, $\lambda * x=\lambda x$ si $\lambda\in k$ et $\gamma * x=\omega^\alpha\gamma(x)$.

On suppose que p divise α.

2) *Alors $\sigma(E)$ est un sous-$k[[\tau]]$-module de E et τ est inversible sur $E/\sigma(E)$ qui devient ainsi un $k((\tau))$-espace vectoriel de dimension finie égale à e_K.*

3) *Sur ce quotient, l'image S_α de l'anneau des entiers $\mathcal{O}_E$ de E est aussi bien un τ-réseau qu'un π_1-réseau.*

L'assertion 1) est évidente. Dans toute la suite on suppose que le nombre p-adique α est divisible par p. Le fait que $\sigma(E)$ est un sous-$k[[\tau]]$-module de E est aussi évident. Pour prouver le reste, nous allons avoir besoin d'un résultat sur les nombres de ramification de l'extension K_∞/K.

5.1. Les nombres de ramification de γ.

Remarquons d'abord que le corps résiduel de E est k sur lequel Γ opère trivialement. En particulier, pour tout $g\in\Gamma$, $(g(\pi)-\pi)/\pi$ appartient à l'idéal maximal de $\mathcal{O}_E$. Notons v la valuation sur E normalisée par

$v(\pi) = 1$. On définit alors les *nombres de ramification de* γ, en posant, pour tout $n \in \mathbb{N}$,

$$i_n(\gamma) = v\Big(\frac{\gamma^{p^n}(\pi)}{\pi} - 1\Big).$$

Comme Γ opère fidèlement sur E, ce sont des entiers ≥ 1. On vérifie que la suite des $i_n(\gamma)$ est strictement croissante et que, si v_p est la valuation p-adique,

$$\forall m \in \mathbb{Z}_p, \quad v\Big(\frac{\gamma^m(\pi)}{\pi} - 1\Big) = i_{v_p(m)}(\gamma).$$

PROPOSITION 5.2. — *Les nombres de ramification de* γ *vérifient* :

1) *pour tout* $n \in \mathbb{N}$, $i_{n+1}(\gamma) \equiv i_n(\gamma) \pmod{p^{n+1}}$;

2) *pour tout* n *suffisamment grand,* $i_{n+1}(\gamma) - i_n(\gamma) = e_K\, p^{n+1}$, *où* e_K *est l'indice de ramification absolu de* K.

Preuve. — Posons $u_0 = i_0(\gamma)$, et pour tout entier $n \geq 1$,

$$u_n = u_{n-1} + \big(i_n(\gamma) - i_{n-1}(\gamma)\big)/p^n.$$

La première assertion signifie que les u_n sont des entiers et la seconde que $u_n - u_{n-1}$ est constant pour n assez grand. Mais, d'après [Win, cor. 3.3.4], les u_n ne sont autres que les nombres de ramification en numérotation supérieure de la $\mathbb{Z}_p$-extension K_∞/K. Alors 1) n'est autre que le théorème de Hasse-Arf (*cf.* [Sel, p. 84]) et 2) est aussi un résultat classique (*cf.* [Wym, § 5]) qui peut s'obtenir soit par la théorie du corps de classes, soit par des calculs un peu pénibles mais élémentaires. □

REMARQUES.

a) En fait, la preuve de ces résultats sur les nombres de ramification de l'extension K_∞/K est beaucoup plus simple dans le cas particulier où nous en avons besoin, celui où K_∞ est la $\mathbb{Z}_p$-extension cyclotomique de K (supposée totalement ramifiée). Lorsque K est le corps obtenu en adjoignant les racines $2p$-ièmes de 1 au corps des fractions de W, un calcul facile montre que, pour tout $n \in \mathbb{N}$, $i_n = p^{n+1} - 1$ si $p \neq 2$ (resp. $p^{n+2} - 1$ si $p = 2$) (*cf.* [Sel, prop. 17, p. 85]) ; le cas général s'en déduit en utilisant le théorème de Herbrand (*cf.* [Sel, p. 82]).

b) L'assertion 1) est aussi un cas particulier d'un théorème de Sen [Sen, th. 1]) valable pour tout « automorphisme sauvagement ramifié » de n'importe quel corps complet pour une valuation discrète à corps résiduel parfait.

COROLLAIRE 5.3. — *On a*

$$\lim_{n\to+\infty} \frac{i_n(\gamma)}{p^n} = \frac{pe_K}{p-1}$$

et pour n suffisamment grand :

$$i_{n+1}(\gamma) < (2p-1)i_n(\gamma).$$

Preuve. — On déduit de 2) qu'il existe un entier N tel que

$$\forall n \geq N, \quad i_n(\gamma) = i_N(\gamma) + p^{N+1}e_K\frac{p^{n-N}-1}{p-1}$$

et la limite est évidente. On a donc, pour n suffisamment grand :

$$\frac{i_n(\gamma)}{p^n} > \frac{pe_K}{2(p-1)},$$

ou encore

$$i_n(\gamma) + e_K p^{n+1} < (2p-1)i_n(\gamma),$$

c'est-à-dire $i_{n+1}(\gamma) < (2p-1)i_n(\gamma)$ si en outre $n \geq N$. □

5.2. Le calcul de $v_0(\tau^s * \bar{x})$ pour $s \in \mathbb{N}$, $\bar{x} \in E/\sigma(E)$.

On note $v_0 : E/\sigma(E) \to \mathbb{Z} \cup \{\infty\}$ l'application définie par :

$$\forall \bar{x} \in E/\sigma(E), \quad v_0(\bar{x}) = \sup\{v(x), x \in \bar{x}\}.$$

Cette borne supérieure est atteinte. Si $\bar{x}$ est non nul, $v_0(\bar{x})$ est un entier premier à p, sinon $v_0(\bar{x})$ est infini.

LEMME 5.4. — *Pour tout entier n premier à p, choisissons un élément $\bar{x}_n$ de $E/\sigma(E)$ tel que $v_0(\bar{x}_n) = n$. Alors tout élément $\bar{x}$ de $E/\sigma(E)$ s'écrit de manière unique sous la forme :*

$$\bar{x} = \sum_{\substack{n \gg -\infty \\ (n,p)=1}} \lambda_n \bar{x}_n, \quad \textit{avec } \lambda_n \in k \textit{ pour tout } n$$

et $v_0(\bar{x})$ est le plus petit entier n tel que $\lambda_n \neq 0$.

Preuve. — Pour tout n premier à p, choisissons un relèvement x_n de $\bar{x}_n$ dans E tel que $v(x_n) = n$; pour tout n divisible par p, posons $x_n = \pi^n$. Alors tout $x \in E$ s'écrit sous la forme $\sum_{n \geq v(x)} \lambda_n x_n$ où les λ_n sont des éléments de k. Par réduction modulo $\sigma(E)$, on obtient l'écriture voulue. Le reste du lemme est évident. □

LEMME 5.5. — *Pour tout $s \in \mathbb{N}$, posons $\omega_s = \prod_{0 \leq i < s} \gamma^i(\omega)$.*

1) *On a $\gamma^s(\pi)/\pi = \omega_s$ et, pour tout $x \in E$, $\gamma^s * x = \omega_s^\alpha \gamma^s(x)$.*

2) *Si s est une puissance de p, pour tout $x \in E$, $\tau^s * x = (\omega_s^\alpha \gamma^s - 1)(x)$.*

Preuve. — L'assertion 1) est immédiate par récurrence sur s et 2) résulte alors de ce que, si s est une puissance de p, on a $\tau^s = (\gamma - 1)^s = (\gamma^s - 1)$ dans $k[[\tau]]$. □

LEMME 5.6. — *Pour tout $n \in \mathbb{Z}_p$ et tout $s \in \mathbb{N}$, on a :*

$$v(\omega_s^n - 1) = p^{v_p(n)}\ i_{v_p(s)}(\gamma).$$

Preuve. — Tout $n \in \mathbb{Z}_p$ s'écrit sous la forme $p^{v_p(n)}m$ avec m unité p-adique. On a alors :

$$v(\omega_s^n - 1) = v\big((\omega_s^m - 1)^{p^{v_p(n)}}\big) = p^{v_p(n)} v(\omega_s^m - 1).$$

Comme m est premier à p, on a $v(\omega_s^m - 1) = v(\omega_s - 1) = i_{v_p(s)}(\gamma)$. □

LEMME 5.7. — *Pour tout $r \in \mathbb{N}$ et tout $x \in E$, on a :*

1) *$v(\tau^{p^r} * x) \geq v(x) + i_r(\gamma)$ avec égalité si $(v(x), p) = 1$.*

2) *$v(\tau^{p^r} * x) \geq v(x) + p i_r(\gamma)$ si $x \in \sigma(E)$.*

Preuve. — D'après le lemme 5.5, pour tout $n \in \mathbb{Z}$, on a $\tau^{p^r} * \pi^n = \omega_{p^r}^\alpha\ (\omega_{p^r}\pi)^n - \pi^n = (\omega_{p^r}^{\alpha+n} - 1)\pi^n$ et, compte-tenu du lemme 5.4, 1) et 2) sont des conséquences immédiates du lemme 5.6. □

LEMME 5.8. — *Soient $x \in E$ et $\bar{x}$ sa classe modulo $\sigma(E)$. Pour tout $s \in \mathbb{N}$:*

1) *Si $p \mid i_0(\gamma)$, alors $v_0(\tau^s * \bar{x}) = v_0(\bar{x}) + s\ i_0(\gamma)$;*

2) *Si p ne divise pas $i_0(\gamma)$, si $i_1(\gamma) < (2p-1)i_0(\gamma)$ et si $v_0(\bar{x}) \equiv i_0(\gamma)$ (mod p), alors $v_0(\tau^s * \bar{x}) = v_0(\bar{x}) + \theta(s)$, où $\theta : \mathbb{Z} \to \mathbb{Z}$ est l'application définie par : pour tout $(q, r) \in \mathbb{Z}^2$, avec $0 \leq r < p - 1$,*

$$\theta\big(q(p-1) + r\big) = q i_1(\gamma) - (q - r) i_0(\gamma).$$

Preuve. — On peut supposer que $\bar{x} \neq 0$, donc que $v_0(\bar{x})$ est un entier premier à p.

1) Soit x un relèvement de $\bar{x}$ dans E tel que $v(x) = v_0(\bar{x})$. Si p divise $i_0(\gamma)$, on voit, par récurrence sur s, que, pour tout $s \in \mathbb{N}$,

$$v(\tau^s * x) = v(x) + s i_0(\gamma)\,;$$

comme c'est un entier premier à p, on a

$$v_0(\overline{\tau^s * x}) = v_0(\tau^s * \bar{x}) = v_0(\bar{x}) + s i_0(\gamma).$$

2) Supposons donc $i_0(\gamma)$ premier à p. En procédant par récurrence, on peut supposer que $s = q(p-1)+r \geq 1$ et que l'assertion est prouvée pour tous les entiers naturels $< s$. Distinguons deux cas :

a) Si $r \neq 0$, on a :

$$v_0(\tau^{s-1} * \bar{x}) = v_0(\bar{x}) + \theta(s-1) = v_0(\bar{x}) + q i_1(\gamma) - (q-r+1) i_0(\gamma).$$

Comme $i_1(\gamma) \equiv i_0(\gamma)$ modulo p, on a

$$v_0(\tau^{s-1} * \bar{x}) \equiv v_0(\bar{x}) + (r-1) i_0(\gamma) \equiv r i_0(\gamma) \not\equiv 0 \pmod{p}$$

et on peut choisir un relèvement z de $\tau^{s-1} * \bar{x}$ dans E tel que $v(z) = v_0(\tau^{s-1} * \bar{x})$. D'après le lemme précédent, on a

$$\begin{aligned} v(\tau * z) &= v(z) + i_0(\gamma) = v_0(\bar{x}) + q i_1(\gamma) - (q-r+1) i_0(\gamma) + i_0(\gamma) \\ &= v_0(\bar{x}) + q i_1(\gamma) - (q-r) i_0(\gamma) \\ &= v_0(\bar{x}) + \theta(s). \end{aligned}$$

Mais cet entier est congru modulo p à $(r+1) i_0(\gamma)$ donc premier à p et on a bien $v_0(\tau^s * \bar{x}) = v_0(\overline{\tau * z}) = v(\tau * z) = v_0(\bar{x}) + \theta(s)$.

b) Si $r = 0$, alors $s \geq p-1$ et

$$v_0(\tau^{s-(p-1)} * \bar{x}) = v_0(\bar{x}) + (q-1)\big(i_1(\gamma) - i_0(\gamma)\big).$$

C'est un entier congru à $i_0(\gamma)$ modulo p donc premier à p et on peut choisir un relèvement y de $\tau^{s-(p-1)} * \bar{x}$ dans E tel que $v(y) = v_0(\tau^{s-(p-1)} * \bar{x})$.

Le lemme précédent nous montre, par récurrence sur n, que pour tout entier n vérifiant $0 \leq n \leq p-1$, $v(\tau^n * y) = v(y) + n\, i_0(\gamma)$. En particulier,

$$v(\tau^{p-1} * y) = v(y) + (p-1) i_0(\gamma) \equiv 0 \pmod{p}.$$

On peut donc écrire $\tau^{p-1} * y = w_0 + w$ avec $w_0 \in \sigma(E)$ et $w \in E$ tels que :

$v(w_0) = v(\tau^{p-1} * y)$,

et ou bien $w = 0$ ou bien $v(w) \not\equiv 0 \pmod{p}$ et $v(w) > v(w_0)$.

On voit que w est un relèvement dans E de $\tau^s * \bar{x}$ et que $v_0(\tau^s * \bar{x}) = v(w)$.

L'assertion 2) du lemme précédent montre que :

$$v(\tau * w_0) \geq v(w_0) + p i_0(\gamma) = v(y) + (2p-1) i_0(\gamma) > v(y) + i_1(\gamma)$$

tandis que l'assertion 1) montre que $v(\tau^p * y) = v(y) + i_1(\gamma)$.

Comme $\tau^p * y = \tau * w_0 + \tau * w$, on a $v(\tau * w) = v(\tau^p * y)$ ou encore

$$v(w) + i_0(\gamma) = v(y) + i_1(\gamma) = v_0(\bar{x}) + q i_1(\gamma) - (q-1) i_0(\gamma).$$

Donc $v_0(\tau^s * \bar{x}) = v(w) = v_0(\bar{x}) + q i_1(\gamma) - q i_0(\gamma) = v_0(\bar{x}) + \theta(s)$. □

5.3. Fin de la preuve du théorème 5.1.

On note E_* le corps E muni de sa structure de $k[[\tau]]$-module définie par l'action $*$.

Compte-tenu du lemme 5.5, la proposition 5.2 et son corollaire nous permettent, quitte à remplacer K par l'extension de degré p^n de K contenue dans L, avec n suffisamment grand et γ par γ^{p^n} de supposer que $i_1(\gamma) - i_0(\gamma) = pe_K$ et que $i_1(\gamma) < (2p-1)i_0(\gamma)$.

Soit $\mathfrak{m}$ l'idéal maximal de l'anneau des entiers de E. Pour tout $t \in \mathbb{Z}$, notons $\overline{\mathfrak{m}}^t$ l'image de l'idéal fractionnaire $\mathfrak{m}^t$ dans le quotient $E/\sigma(E)$.

On distingue alors deux cas :

a) *Le cas où p divise $i_0(\gamma)$.* — On voit, par récurrence sur $s \in \mathbb{N}$, que $v(\tau^s(\pi)) = 1 + si_0(\gamma)$, d'où l'on déduit que $i_n(\gamma) = p^n i_0(\gamma)$ pour tout entier naturel n. La suite des $i_n(\gamma)/p^n$ est donc constante et, d'après le corollaire 5.2, $i_0(\gamma) = pe_K/(p-1)$.

On en déduit que l'ensemble I des entiers i premiers à p tels que $0 < i < i_0(\gamma)$ a e_K éléments.

Pour $t \in \mathbb{Z}$, $i \in I$ et $s \in \mathbb{N}$, posons :

$$\nu_{i,s}^t = pt + i + si_0(\gamma).$$

Pour t fixé, on voit que les entiers $\nu_{i,s}^t$ sont deux à deux distincts et parcourent l'ensemble des entiers premiers à p supérieurs à pt.

Comme, pour tout $i \in I$ et tout $t \in \mathbb{Z}$, $pt + i$ est premier à p, l'assertion 1) du lemme 5.8 montre que :

$$\forall s \in \mathbb{N},\ \forall i \in I,\ \forall t \in \mathbb{Z}, \quad v_0(\tau^s * \overline{\pi^{pt+i}}) = pt + i + s\, i_0(\gamma) = \nu_{i,s}^t.$$

On en déduit, en appliquant le lemme 5.4, que pour tout $t \in \mathbb{Z}$:

(i) *le sous-$k[[\tau]]$-module M_t de $E_*/\sigma(E_*)$ engendré par les $(\overline{\pi^{pt+i}})_{i\in I}$ est libre de rang e_K ;*

(ii) $M_t = \overline{\mathfrak{m}}^{pt}$ *et* $\tau * (M_t) = M^{t+i_0(\gamma)/p}$.

Comme $E_*/\sigma(E_*)$ est la réunion des M_t, le théorème 5.1 s'en déduit facilement.

b) *Le cas où p ne divise pas $i_0(\gamma)$.* — Posons cette fois-ci

$$I = \{i \in \mathbb{Z} \mid i \equiv i_0(\gamma) \pmod{p} \text{ et } i_0(\gamma) \leq i < i_0(\gamma) + e_K p\}.$$

C'est encore un ensemble à e_K éléments.

Pour $t \in \mathbb{Z}$, $i \in I$ et $s \in \mathbb{N}$, posons :

$$\nu_{i,s}^t = pt + i + \theta(s).$$

Si $s \in \mathbb{N}$ et si $s = q(p-1) + r$ est la division euclidienne de s par $p-1$, on a :

$$\theta(s) = qi_1(\gamma) - (q-r)i_0(\gamma) = qpe_K + r\ i_0(\gamma).$$

On en déduit que, pour t fixé, la famille des $\nu_{i,s}^t$ est en bijection avec celle des

$$\mu_{i,q,r}^t = pt + i + qpe_K + r\ i_0(\gamma),$$

pour $i \in I$, $q \in \mathbb{N}$ et $r \in \mathbb{N}$ vérifiant $0 \leq r < p-1$.

On vérifie qu'ici encore, pour t fixé, ces entiers sont deux à deux distincts et sont tous premiers à p. L'assertion 2) du lemme 5.8 montre que

$$\forall s \in \mathbb{N},\ \forall i \in I,\ \forall t \in \mathbb{Z}, \quad v_0(\tau^s * \overline{\pi^{pt+i}}) = pt + i + \theta(s) = \nu_{i,s}^t$$

et donc que

(i) *le sous-$k[[\tau]]$-module M_t de $E_*/\sigma(E_*)$ engendré par les $(\overline{\pi^{pt+i}})_{i\in I}$ est libre de rang e_K.*

En regardant les valeurs prises par les entiers $\mu_{i,q,r}^t$, on vérifie aussi que

(ii) *M_t est contenu dans $\overline{\mathfrak{m}}^{pt+i_0(\gamma)}$ et contient $\overline{\mathfrak{m}}^{pt+p\ i_0(\gamma)}$. De plus, $\tau * (M_t)$ contient $\overline{\mathfrak{m}}^{p(t+e_K+i_0(\gamma))}$.*

Ici encore $E_*/\sigma(E_*)$ est la réunion des M_t et le théorème 5.1 s'en déduit.

BIBLIOGRAPHIE

[Fo1] FONTAINE (J.-M.). — *Représentations p-adiques des corps locaux.* — The Grothendieck Festschrift, Birkhäuser, Boston, t. **2**, 1991, p. 249–309.

[Fo2] FONTAINE (J.-M.). — *Le corps des périodes p-adiques, exposé séminaire I.H.E.S. 1988, Périodes p-adiques*, Astérisque 223, 1994, p. 59–111.

[Mil] MILNE (J.S.). — *Arithmetic duality theorems*, Perspectives in Math., Academic Press, t. **1**, 1986.

[Poi] POITOU (G.). — *Cohomologie galoisienne des modules finis*, Dunod.

[Sen] SEN (S.) On automorphisms of local fields. — Ann. of Math. (2), t. **90**, 1969, p. 33–46.

[Se1] SERRE (J.-P.). — *Corps locaux*, 2e éd. — Hermann, 1968.

[Se2] SERRE (J.-P.). — *Cohomologie Galoisienne*, 5e éd, Lecture Notes Math., Springer, t. **5**, 1994.

[Tat] TATE (J.). — *Duality theorems in Galois cohomology over number fields*. — Proc. Int. Congress Math. Stokholm, 1962, p. 288–295.

[Wac] WACH (N.). — *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France, t. **124**, 1996, p. 375–400.

[Win] WINTENBERGER (J.-P.). — *Le corps des normes de certaines extensions infinies de corps locaux; applications*, Ann. Sci. École Normale Supérieure (4), t. **16**, 1983, p. 59–89.

[Wym] WYMAN (B.F.). — *Wildly ramified gamma extensions*, Amer. J. Math., t. **91**, 1969, p. 135–152.