REPRÉSENTATIONS CRISTALLINES ET REPRÉSENTATIONS DE HAUTEUR FINIE

par

Pierre Colmez

Résumé. — Nous prouvons que les représentations absolument cristallines sont de hauteur finie, ainsi que Fontaine l'avait conjecturé.

Abstract. — We prove that absolutely crystalline representations are of finite height, as was conjectured by Fontaine.

Table des matières

Introduction.

Ce travail s'inscrit dans le cadre de la classification, introduite par Fontaine [**10**], des représentations p-adiques du groupe de Galois absolu $\mathscr{G}_K$ d'une extension finie K de $\mathbf{Q}_p$ en termes de (φ, Γ)-modules. Le point essentiel de la classification de Fontaine est que l'on peut reconstruire une représentation V à partir de son (φ, Γ)-module $D(V)$ et que l'on doit donc être capable de lire sur ce module les propriétés de la représentation ; l'idée étant que plus la représentation est "sympathique", plus son (φ, Γ)-module doit être "sympathique". Dans cet article, nous démontrons que les représentations absolument cristallines sont aussi sympathiques que possibles. Plus précisément, nous démontrons le résultat suivant conjecturé par Fontaine.

Théorème .1. — *Si K est une extension non ramifiée de $\mathbf{Q}_p$ et V est une représentation cristalline de $\mathscr{G}_K$, alors V est de hauteur finie.*

La notion de "représentation de hauteur finie" a été introduite par Fontaine [**10**] et étudiée en détails par Wach [**16**] et [**15**] qui a en particulier démontré le théorème précédent dans le cas où les poids de Hodge-Tate de la représentation sont dans un intervalle de longueur $p-1$ grâce à une démonstration des résultats de Fontaine-Lafaille [**8**] via la théorie des (φ, Γ)-modules.

La démonstration du théorème se fait en trois étapes. On commence par utiliser le fait que toute représentation est surconvergente [**3**]. Ceci nous permet d'appliquer les résultats de [**4**] sur la comparaison entre deux constructions d'un inverse de l'application exponentielle de Perrin-Riou [**14**] et [**5**] pour démontrer qu'une représentation absolument cristalline et surconvergente a un (φ, Γ)-module qui est presque de hauteur finie. Puis on démontre qu'un (φ, Γ)-module qui est presque de hauteur finie est en fait de hauteur finie et on conclut en utilisant un résultat de Fontaine disant qu'une représentation dont le (φ, Γ)-module est de hauteur finie est elle-même de hauteur finie.

La démonstration du théorème est donc assez détournée ; il serait très agréable d'en trouver une plus directe d'autant plus que cela permettrait probablement de démontrer du même coup la conjecture "faiblement admissible implique admissible" dans le cas non ramifié du moins.

Signalons que Benois [**1**] a entrepris le chemin inverse et obtenu une démonstration de la loi de réciprocité explicite de Perrin-Riou (ce qui revient plus ou moins à comparer les deux constructions de l'inverse de l'exponentielle de Perrin-Riou auxquelles il a été fait allusion plus haut) dans le cas d'une représentation cristalline de hauteur finie.

I. Anneaux de Fontaine et représentations p-adiques.

Nous renvoyons aux articles [**10**], [**11**] et [**12**] pour la démonstration de la plupart des faits rappelés sans référence précise dans ce chapitre.

1. Notations générales.— On se fixe une clôture algébrique $\overline{\mathbf{Q}}_p$ de $\mathbf{Q}_p$ et toutes les extensions finies de $\mathbf{Q}_p$ que nous aurons à considérer seront supposées être des sous-corps de $\overline{\mathbf{Q}}_p$. On note $\mathscr{G}_{\mathbf{Q}_p}$ le groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ et $\chi : \mathscr{G}_{\mathbf{Q}_p} \to \mathbf{Z}_p^*$ le caractère cyclotomique.

Si K est une extension finie de $\mathbf{Q}_p$ et $n \in \mathbf{N}$, on pose $K_n = K(\mu_{p^n}) \subset \overline{\mathbf{Q}}_p$ et on note K_∞ l'extension cyclotomique de K réunion des K_n. On note aussi $\mathscr{G}_K$ le groupe de galois $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$

et $\mathscr{H}_K$ le noyau de la restriction de χ à $\mathscr{G}_K$. On a $\mathscr{H}_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty)$ et on pose $\Gamma_K = \mathscr{G}_K/\mathscr{H}_K = \mathrm{Gal}(K_\infty/K)$.

2. Le corps $\widetilde{\mathbf{E}}$ et certains de ses sous-anneaux.— Soit $\mathbf{C}_p$ le complété de $\overline{\mathbf{Q}}_p$ pour la topologie p-adique. Soit $\widetilde{\mathbf{E}}$ l'ensemble des suites $x = (x^{(0)}, \dots, x^{(n)}, \dots)$ d'éléments de $\mathbf{C}_p$ vérifiant $(x^{(n+1)})^p = x^{(n)}$. On munit $\widetilde{\mathbf{E}}$ des lois $+$ et $\cdot$ définies par $x + y = s$ où $s^{(n)} = \lim_{m\to+\infty}(x^{(n+m)} + y^{(n+m)})^{p^m}$ et $x \cdot y = t$, avec $t^{(n)} = x^{(n)}y^{(n)}$, ce qui fait de $\widetilde{\mathbf{E}}$ un corps de caractéristique p algébriquement clos et complet pour la valuation $v_{\mathbf{E}}$ définie par $v_{\mathbf{E}}(x) = v_p(x^{(0)})$. On note $\widetilde{\mathbf{E}}^+$ l'anneau des entiers de $\widetilde{\mathbf{E}}$ (cet anneau est noté R ou $\mathscr{R}$ dans la théorie des représentations de de Rham).

Soit $\varepsilon = (1, \varepsilon^{(1)}, \dots, \varepsilon^{(n)} \dots)$ un élément de $\widetilde{\mathbf{E}}$ tel que $\varepsilon^{(1)} \neq 1$, ce qui implique que si $n \geqslant 1$, alors $\varepsilon^{(n)}$ est une racine primitive p^n-ième de l'unité. On a $v_{\mathbf{E}}(\varepsilon - 1) = \frac{p}{p-1}$ et on note $\mathbf{E}_{\mathbf{Q}_p}$ le sous-corps $\mathbf{F}_p((\varepsilon - 1))$ de $\widetilde{\mathbf{E}}$. On note $\mathbf{E}$ la clôture séparable de $\mathbf{E}_{\mathbf{Q}_p}$ dans $\widetilde{\mathbf{E}}$ et $\mathbf{E}^+$ (resp. $\mathfrak{m}_{\mathbf{E}}$) l'anneau de ses entiers (resp. l'idéal maximal de $\mathbf{E}^+$). Le corps $\mathbf{E}$ est stable par l'action de $\mathscr{G}_{\mathbf{Q}_p}$ et $E^{\mathscr{H}_{\mathbf{Q}_p}} = E_{\mathbf{Q}_p}$. La théorie du corps des normes ([**7**] et [**17**]) permet de montrer que $\mathbf{E}_K = \mathbf{E}^{\mathscr{H}_K}$ est une extension finie séparable de $\mathbf{E}_{\mathbf{Q}_p}$ de degré $\mathscr{H}_{\mathbf{Q}_p}/\mathscr{H}_K = [K_\infty : \mathbf{Q}_p(\mu_{p^\infty})]$, ce qui permet aussi d'identifier $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_K)$ avec $\mathscr{H}_K$. On notera $\mathbf{E}_K^+ = \mathbf{E}_K \cap \mathbf{E}^+$ l'anneau des entiers de $\mathbf{E}_K$.

3. Le corps $\widetilde{\mathbf{B}}$ et certains de ses sous-anneaux.— Soit $\widetilde{\mathbf{A}} = W(\widetilde{\mathbf{E}})$ l'anneau des vecteurs de Witt à coefficients dans $\widetilde{\mathbf{E}}$ et $\widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}[\frac{1}{p}] = \mathrm{Fr}(\widetilde{\mathbf{A}})$, ce qui fait de $\widetilde{\mathbf{B}}$ un corps muni d'une valuation discrète complet, d'anneau de valuation $\widetilde{\mathbf{A}}$ et de corps résiduel $\widetilde{\mathbf{E}}$. Si $x \in \widetilde{\mathbf{E}}$, on note $[x]$ son représentant de Teichmüller dans $\widetilde{\mathbf{A}}$. Tout élément x de $\widetilde{\mathbf{A}}$ s'écrit donc de manière unique sous la forme $\sum_{k=0}^{+\infty} p^k[x_k]$ et tout élément de $\widetilde{\mathbf{B}}$ sous la forme $\sum_{k\gg-\infty}^{+\infty} p^k[x_k]$.

On munit $\widetilde{\mathbf{A}}$ de la topologie qui fait de l'application $x \to (x_k)_{k\in\mathbf{N}}$ un homéomorphisme de $\widetilde{\mathbf{A}}$ sur $\widetilde{\mathbf{E}}^{\mathbf{N}}$ muni de la topologie produit ($\widetilde{\mathbf{E}}$ étant muni de la topologie définie par la valuation $v_{\mathbf{E}}$) et on munit $\widetilde{\mathbf{B}} = \bigcup_{n\in\mathbf{N}} p^{-n}\widetilde{\mathbf{A}}$ de la topologie de la limite inductive. L'action de $\mathscr{G}_{\mathbf{Q}_p}$ sur $\widetilde{\mathbf{E}}$ se prolonge en une action continue sur $\widetilde{\mathbf{A}}$ et $\widetilde{\mathbf{B}}$ qui commute à celle du morphisme de Frobenius φ.

Soit $\pi = [\varepsilon] - 1$. Soit $\mathbf{A}_{\mathbf{Q}_p}$ l'adhérence dans $\widetilde{\mathbf{A}}$ de $\mathbf{Z}_p[\pi, \frac{1}{\pi}]$. C'est l'ensemble des éléments de $\widetilde{\mathbf{A}}$ de la forme $\sum_{n\in\mathbf{Z}} a_n\pi^n$ où a_n est une suite d'éléments de $\mathbf{Z}_p$ tendant vers 0 quand n tend vers $-\infty$. L'anneau $\mathbf{A}_{\mathbf{Q}_p}$ est un anneau de valuation discrète complet de corps résiduel $\mathbf{E}_{\mathbf{Q}_p}$. Comme

$$\varphi(\pi) = (1+\pi)^p - 1 \quad \text{et} \quad g(\pi) = (1+\pi)^{\chi(g)} - 1 \text{ si } g \in \mathscr{G}_{\mathbf{Q}_p},$$

l'anneau $\mathbf{A}_{\mathbf{Q}_p}$ et son corps des fractions $\mathbf{B}_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p}[\frac{1}{p}]$ sont stables par φ et $\mathscr{G}_{\mathbf{Q}_p}$.

On note $\mathbf{B}$ l'adhérence de l'extension maximale non ramifiée de $\mathbf{B}_{\mathbf{Q}_p}$ contenue dans $\widetilde{\mathbf{B}}$ et $\mathbf{A} = \mathbf{B} \cap \widetilde{\mathbf{A}}$ de telle sorte que l'on a $\mathbf{B} = \mathbf{A}[\frac{1}{p}]$, que $\mathbf{A}$ est un anneau de valuation discrète complet dont le corps des fractions est $\mathbf{B}$ et le corps résiduel est $\mathbf{E}$. L'anneau $\mathbf{A}$ et le corps $\mathbf{B}$ sont stables par φ et $\mathscr{G}_{\mathbf{Q}_p}$.

Si K est une extension finie de $\mathbf{Q}_p$, on pose $\mathbf{A}_K = \mathbf{A}^{\mathscr{H}_K}$ et $\mathbf{B}_K = \mathbf{B}^{\mathscr{H}_K}$, ce qui fait de $\mathbf{A}_K$ un anneau de valuation discrète complet de corps résiduel $\mathbf{E}_K$ et de corps des fractions $\mathbf{B}_K = \mathbf{A}_K[\frac{1}{p}]$. D'autre part, si $K = \mathbf{Q}_p$, les deux définitions de $\mathbf{A}_K$ et $\mathbf{B}_K$ coincident.

Si L est une extension finie de K, $\mathbf{B}_L$ est une extension non ramifiée de $\mathbf{B}_K$ de degré $[L_\infty : K_\infty]$. Si l'extension L/K est de plus supposée galoisienne, alors les extensions $\widetilde{\mathbf{B}}_L/\widetilde{\mathbf{B}}_K$ et $\mathbf{B}_L/\mathbf{B}_K$ sont aussi galoisiennes de groupe de Galois $\mathrm{Gal}(\widetilde{\mathbf{B}}_L/\widetilde{\mathbf{B}}_K) = \mathrm{Gal}(\mathbf{B}_L/\mathbf{B}_K) = \mathrm{Gal}(\mathbf{E}_L/\mathbf{E}_K) = \mathrm{Gal}(L_\infty/K_\infty) = \mathscr{H}_K/\mathscr{H}_L$.

4. Le (φ, Γ_K)-module associé à une représentation de $\mathscr{G}_K$.

Définition I.1. — *i) On appelle $\mathbf{Z}_p$-représentation de $\mathscr{G}_K$, un $\mathbf{Z}_p$-module de type fini muni d'une action $\mathbf{Z}_p$-linéaire continue de $\mathscr{G}_K$.*

ii) On appelle représentation p-adique de $\mathscr{G}_K$ tout $\mathbf{Q}_p$-espace vectoriel de dimension finie muni d'une action linéaire continue de $\mathscr{G}_K$

Définition I.2. — *Si K est une extension finie de $\mathbf{Q}_p$, on appelle (φ, Γ_K)-module sur $\mathbf{A}_K$ (resp. $\mathbf{B}_K$) tout $\mathbf{A}_K$-module de type fini (resp. tout $\mathbf{B}_K$-espace vectoriel de dimension finie) muni d'une action de Γ_K et d'une action de φ commutant à celle de Γ_K.*

Si K est une extension finie de $\mathbf{Q}_p$ et V est une $\mathbf{Z}_p$-représentation ou une représentation p-adique de $\mathscr{G}_K$, on pose
$$D(V) = (\mathbf{A} \otimes_{\mathbf{Z}_p} V)^{\mathscr{H}_K}.$$
L'action de φ sur $\mathbf{A}_K$ commutant à celle de $\mathscr{G}_K$, $D(V)$ est muni d'une action de φ qui commute à l'action résiduelle de $\mathscr{G}_K/\mathscr{H}_K = \Gamma_K$, ce qui fait de $D(V)$ un (φ, Γ_K)-module sur $\mathbf{A}_K$ ou $\mathbf{B}_K$ suivant que V est une $\mathbf{Z}_p$-représentation ou une représentation p-adique de $\mathscr{G}_K$. Si V est une représentation p-adique de $\mathscr{G}_K$ de dimension d, le (φ, Γ_K)-module $D(V)$ est étale, c'est-à-dire qu'il existe une base de $D(V)$ sur $\mathbf{B}_K$ dans laquelle la matrice de φ appartient à $\mathrm{GL}_d(A)$.

D'autre part, si V est une $\mathbf{Z}_p$-représentation ou une représentation p-adique de $\mathscr{G}_K$, alors $(\mathbf{A} \otimes_{\mathbf{A}_K} D(V))^{\varphi=1}$ est canoniquement isomorphe à V en tant que représentation de $\mathscr{G}_K$. En d'autres termes, V est déterminée par son (φ, Γ_K)-module $D(V)$. En particulier, si V est une représentation p-adique de $\mathscr{G}_K$, on a $\dim_{\mathbf{B}_K} D(V) = \dim_{\mathbf{Q}_p} V$ et l'application naturelle de $\mathbf{B} \otimes_{\mathbf{B}_K} D(V) \longrightarrow \mathbf{B} \otimes_{\mathbf{Q}_p} V$ est un isomorphisme. Les coefficients de la matrice de cet isomorphisme dans des bases de V sur $\mathbf{Q}_p$ et $D(V)$ sur $\mathbf{B}_K$ s'appellent les périodes de la représentation V et le problème qui se pose est d'arriver à lire les propriétés d'une représentation sur ses périodes.

5. Représentations de de Rham et cristallines.— Soit $\widetilde{\mathbf{A}}^+ = W(\widetilde{\mathbf{E}}^+)$ l'anneau des vecteurs de Witt à coefficients dans $\widetilde{\mathbf{E}}^+$ (c'est l'anneau $W(R)$ de **[9]** ou $\mathbf{A}_{\mathrm{inf}}$ de **[11]**) et si $x \in \widetilde{\mathbf{E}}^+$, soit $[x]$ son représentant de Teichmüller dans $\widetilde{\mathbf{A}}^+$.

L'homomorphisme θ de $\widetilde{\mathbf{A}}^+$ dans $\mathscr{O}_{\mathbf{C}_p}$ qui à $\sum_{n=0}^{+\infty} p^n [x_n]$ associe $\sum_{n=0}^{+\infty} p^n x_n^{(0)}$ est surjectif et son noyau est un idéal principal engendré par $\omega = \frac{\pi}{\varphi^{-1}(\pi)}$. On prolonge θ en un morphisme de $\widetilde{\mathbf{B}}^+ = \widetilde{\mathbf{A}}[\frac{1}{p}]$ sur $\mathbf{C}_p$, on note $\mathbf{B}_{\mathrm{dR}}^+$ l'anneau $\varprojlim \widetilde{\mathbf{B}}^+/(\ker\theta)^n$ et on prolonge θ par continuité en un morphisme de $\mathbf{B}_{\mathrm{dR}}^+$ sur $\mathbf{C}_p$. Ceci fait de $\mathbf{B}_{\mathrm{dR}}^+$ un anneau de valuation discrète d'idéal maximal $\ker\theta$ et de corps résiduel $\mathbf{C}_p$. L'action de $\mathscr{G}_{\mathbf{Q}_p}$ sur $\widetilde{\mathbf{B}}^+$ s'etend par continuité en une action continue de $\mathscr{G}_{\mathbf{Q}_p}$ sur $\mathbf{B}_{\mathrm{dR}}^+$. La série $\log[\varepsilon] = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} \pi^n$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$ vers un élément que nous noterons t, qui est un générateur de $\ker\theta$ sur lequel $\sigma \in \mathscr{G}_{\mathbf{Q}_p}$ agit via la formule $\sigma(t) = \chi(\sigma)t$ et qui peut être vu comme un analogue p-adique de $2i\pi$. On note $\mathbf{B}_{\mathrm{dR}} = \mathbf{B}_{\mathrm{dR}}^+[t^{-1}]$ le corps des fractions de $\mathbf{B}_{\mathrm{dR}}^+$.

Soit K une extension finie de $\mathbf{Q}_p$. Soit V une représentation p-adique de $\mathscr{G}_K$. Le K-espace vectoriel $D_{\mathrm{dR}}(V) = (\mathbf{B}_{\mathrm{dR}} \otimes V)^{\mathscr{G}_K}$ est de dimension inférieure ou égale à celle de V sur $\mathbf{Q}_p$. On dit que V est de de Rham s'il y a égalité.

Soit $\mathbf{A}_{\mathrm{cris}}$ l'ensemble des $x \in \mathbf{B}_{\mathrm{dR}}^+$ tels qu'il existe une suite $(a_n)_{n\in\mathbf{N}}$ d'éléments de $\widetilde{\mathbf{A}}^+$ tendant vers 0 telle que l'on ait $x = \sum_{n=0}^{+\infty} a_n \frac{\omega^n}{n!}$. Alors $\mathbf{B}_{\mathrm{cris}}^+ = \mathbf{A}_{\mathrm{cris}}[\frac{1}{p}]$ est un sous-anneau de $\mathbf{B}_{\mathrm{dR}}^+$ stable par $\mathscr{G}_{\mathbf{Q}_p}$ contenant t et l'action de φ sur $\widetilde{\mathbf{B}}^+$ s'étend par continuité en une action sur $\mathbf{B}_{\mathrm{cris}}^+$. On a $\varphi(t) = pt$ et on note $\mathbf{B}_{\mathrm{cris}}$ le sous-anneau $\mathbf{B}_{\mathrm{cris}}^+[\frac{1}{t}]$ de $\mathbf{B}_{\mathrm{dR}}$.

Si $F = K \cap \mathbf{Q}_p^{\mathrm{nr}}$, le F-espace vectoriel $D_{\mathrm{cris}}(V) = (\mathbf{B}_{\mathrm{cris}} \otimes V)^{\mathscr{G}_K}$ est aussi de dimension inférieure où égale à celle de V sur $\mathbf{Q}_p$ et on dit que V est cristalline s'il y a égalité. L'action de φ sur $\mathbf{B}_{\mathrm{cris}}$ commutant à celle de $\mathscr{G}_K$, ceci munit naturellement $D_{\mathrm{cris}}(V)$ d'une action semi-linéaire (relativement à la structure de $K \cap \mathbf{Q}_p^{\mathrm{nr}}$-espace vectoriel) de φ.

6. Représentations de hauteur finie : énoncé du résultat principal. — Une représentation est dite de hauteur finie si ses périodes n'ont pas de dénominateur (en π) du tout. De manière précise, soient $\mathbf{A}^+ = \mathbf{A} \cap \widetilde{\mathbf{A}}^+ = \mathbf{B} \cap \widetilde{\mathbf{A}}^+$ et $\mathbf{B}^+ = \mathbf{A}^+[\frac{1}{p}]$. Si K est une extension finie de $\mathbf{Q}_p$, on pose $\mathbf{A}_K^+ = (\mathbf{A}^+)^{\mathscr{H}_K}$ et $\mathbf{B}_K^+ = (\mathbf{B}^+)^{\mathscr{H}_K} = \mathbf{A}_K^+[\frac{1}{p}]$ et, si k_K est le corps résiduel de K, on a $\mathbf{A}_K^+ = W(k_K)[[\pi]]$ (cf. [**15**]).

Définition I.3. — *Si K est une extension finie de $\mathbf{Q}_p$ et V est une représentation p-adique de $\mathscr{G}_K$, on pose*

$$D^+(V) = (\mathbf{A}^+ \otimes_{\mathbf{Z}_p} V)^{\mathscr{H}_K}.$$

On dit que V est de hauteur finie si $D(V)$ possède une base sur $\mathbf{B}_K$ constituée d'éléments de $D^+(V)$.

Le reste de cet article va être consacré à la démonstration du résultat suivant.

Théorème I.4. — *Si K est non ramifiée sur $\mathbf{Q}_p$ et V est une représentation p-adique de $\mathscr{G}_K$ de dimension d, les deux conditions suivantes sont équivalentes.*

i) V est cristalline

ii) V est de hauteur finie et il existe $r \in \mathbf{Z}$ et un sous-$\mathbf{B}_K^+$-module N de $D(V)$ de rang d stable par Γ_K et φ tel que Γ_K agisse trivialement sur $(N/\pi N)(r)$.

Remarque I.5. — Le cadre naturel pour énoncer ce résultat est de supposer seulement que K est le corps des fractions de l'anneau des vecteurs de Witt à coefficients dans un corps parfait de caractéristique p (i.e. ne pas imposer au corps résiduel d'être fini). Le lecteur se convaincra aisément que les démonstrations effectuées dans cet article s'étendent au cas général. Le problème pour étendre le résultat est que la démonstration utilise fortement des résultats de [**4, 5**] qui ne sont rédigés que dans le cas d'un corps résiduel fini. Étendre les résultats de [**4**] ne pose pas vraiment de problème, mais pour pouvoir utiliser ceux de [**5**] rappelés dans la proposition II.7, on a besoin de la surjectivité (après torsion à la Tate) de l'exponentielle de Bloch-Kato et la démonstration de cette surjectivité [**2**] repose sur un argument de dimensions qui ne marche que quand le corps résiduel est fini (sans cette surjectivité, la condition $(*)$ de la proposition II.7 pourrait très bien n'être jamais satisfaite).

Remarque I.6. — Wach a construit des exemples de représentations cristallines, dans le cas où K est ramifié sur $\mathbf{Q}_p$, qui ne sont pas de hauteur finie et ce que l'on est en droit d'attendre d'une représentation cristalline dans le cas général n'est pas clair pour le moment. D'autre part, l'implication ii)⇒i) et l'existence de N et r si V est cristalline et de hauteur finie découlent de la proposition I.7 ci-dessous dont on peut trouver la démonstration dans [**15**] ; pour démontrer le théorème, il suffit donc de montrer que si V est cristalline, alors V est de hauteur finie, ce qui sera fait aux chapitres II et III.

Proposition I.7. — *Si K est une extension finie de $\mathbf{Q}_p$ et V est une représentation p-adique de $\mathscr{G}_K$ de hauteur finie, les deux conditions suivantes sont équivalentes.*

i) V est cristalline.

ii) Il existe $r \in \mathbf{Z}$ et un sous $\mathbf{B}_K^+$-module N de $D^+(V)$ libre de rang $d = \dim_{\mathbf{Q}_p} V$ stable par Γ_K et φ tels que Γ_K agisse trivialement sur $(N/\pi N)(r)$.

7. Généralités sur les représentations surconvergentes.— Pour passer de la théorie des (φ, Γ_K)-modules à celle des représentations de de Rham, on doit se restreindre aux représentations dont les périodes vivent naturellement à la fois dans $\mathbf{B}_{\mathrm{dR}}$ et $\mathbf{B}$.

Tout élément x de $\widetilde{\mathbf{B}}$ peut s'écrire de manière unique comme somme d'une série du type $\sum_{k\gg-\infty} p^k[x_k]$, où les x_k sont des éléments de $\widetilde{\mathbf{E}}$ et la série converge (cf. proposition II.25) dans $\mathbf{B}_{\mathrm{dR}}^+$ si et seulement si la série $\sum_{k\gg-\infty} p^k x_k^{(0)}$ converge dans $\mathbf{C}_p$ c'est-à-dire si et seulement si $k+v_{\mathbf{E}}(x_k)$ tend vers $+\infty$ quand k tend vers $+\infty$. Plus généralement, si $n \in \mathbf{N}$, la série définissant $\varphi^{-n}(x)$ converge si et seulement si $k + p^{-n}v_{\mathbf{E}}(x_k)$ tend vers $+\infty$ quand k tend vers $+\infty$.

Un élément x de $\widetilde{\mathbf{B}}$ tel qu'il existe $n \in \mathbf{N}$ tel que la série définissant $\varphi^{-n}(x)$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$ sera dit surconvergent. On note $\widetilde{\mathbf{B}}^\dagger$ l'ensemble des éléments surconvergents de $\widetilde{\mathbf{B}}$; c'est un sous-corps de $\widetilde{\mathbf{B}}$ stable par φ et $\mathscr{G}_K$. Si $n \in \mathbf{N}$, on note $\widetilde{\mathbf{B}}^{\dagger,n}$ l'ensemble des $x \in \widetilde{\mathbf{B}}$ tels que $\varphi^{-n}(x)$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$; c'est un sous-anneau de $\widetilde{\mathbf{B}}$ stable par $\mathscr{G}_{\mathbf{Q}_p}$ et on a $\widetilde{\mathbf{B}}^\dagger = \bigcup_{n\in\mathbf{N}} \widetilde{\mathbf{B}}^{\dagger,n}$.

On définit un sous-corps $\mathbf{B}^\dagger$ de $\mathbf{B}$ stable par φ et $\mathscr{G}_{\mathbf{Q}_p}$ et, si $n \in \mathbf{N}$, un sous-anneau $\mathbf{B}^{\dagger,n}$ de $\mathbf{B}$ stables par $\mathscr{G}_K$ en posant $\mathbf{B}^\dagger = \mathbf{B} \cap \widetilde{\mathbf{B}}^\dagger$ et $\mathbf{B}^{\dagger,n} = \mathbf{B} \cap \widetilde{\mathbf{B}}^{\dagger,n}$. Par construction, $\varphi^{-n}(\mathbf{B}^{\dagger,n})$ s'identifie naturellement à un sous-anneau de $\mathbf{B}_{\mathrm{dR}}^+$. Finalement, si K est une extension finie de $\mathbf{Q}_p$, on pose $\mathbf{B}_K^\dagger = (\mathbf{B}^\dagger)^{\mathscr{H}_K}$ et $\mathbf{B}_K^{\dagger,n} = (\mathbf{B}^{\dagger,n})^{\mathscr{H}_K}$

Si V est une représentation p-adique de $\mathscr{G}_K$, on pose

$$D^\dagger(V) = (\mathbf{B}^\dagger \otimes_{\mathbf{Q}_p} V)^{\mathscr{H}_K} \quad \text{et} \quad D^{\dagger,n}(V) = (\mathbf{B}^{\dagger,n} \otimes_{\mathbf{Q}_p} V)^{\mathscr{H}_K} \text{ si } n \in \mathbf{N}.$$

Proposition I.8. — *i) Le $\mathbf{B}_K^\dagger$-espace vectoriel $D^\dagger(V)$ est de dimension $\dim_{\mathbf{Q}_p} V$ et contient une base de $D(V)$ sur $\mathbf{B}_K$.*

ii) La matrice de φ dans une base de $D(V)$ constituée d'éléments de $D^\dagger(V)$ appartient à $\mathrm{GL}_d(\mathbf{B}_K^\dagger)$.

Démonstration. — Le i) est le résultat principal de [**3**] (toute représentation p-adique de $\mathscr{G}_K$ est surconvergente) et le ii) est une conséquence du fait que $D^\dagger(V)$ est stable par φ puisque φ envoie $D^{\dagger,n}(V)$ dans $D^{\dagger,n+1}(V)$.

II. Les représentations absolument cristallines sont presque de hauteur finie.

Ce chapitre est consacré à la démonstration de son titre et plus précisément à la proposition II.1 ci-dessous (l'opérateur ψ sur $D(V)$ est un inverse à gauche de φ et est défini au §2).

Proposition II.1. — *Si K est une extension finie non ramifiée de $\mathbf{Q}_p$ et V une représentation cristalline de $\mathscr{G}_K$ de dimension d, on peut trouver un sous-groupe ouvert Γ de Γ_K et une base $e_1, \dots, e_d$ de $D(V)$ sur $\mathbf{B}_K$ constituée d'éléments de $D(V)^{\psi=1}$ tels que le sous-*$\mathrm{Fr}(\mathbf{B}_K^+)$*-espace vectoriel de $D(V)$ engendré par $e_1 \dots, e_d$, soit stable par φ et Γ.*

1. Quelques anneaux de séries de Laurent.— Pour faire le lien entre les représentations cristallines et les représentations surconvergentes, nous allons avoir besoin d'introduire un certain nombre d'anneaux de séries de Laurent en une variable T qui permettent de décrire de manière un peu plus agréable les anneaux $\mathbf{B}_K^{\dagger,n}$, $\mathbf{B}_K$ et $\mathbf{B}_K^+$.

Soit K une extension finie de $\mathbf{Q}_p$. Si $r \in \mathbf{R}_+$, on note $\mathscr{B}_K^{r[}$ (resp. $\mathscr{B}_K^{r)}$, resp. $\mathscr{B}_K^{r]}$) l'ensemble des séries de Laurent de la forme $\sum_{n\in\mathbf{Z}} a_n T^n$ à coefficients dans K telles que la suite de terme général $|a_n|\rho^n$ tend vers 0 quand n tend vers $+\infty$ quel que soit $\rho < r$ (resp. la suite $(|a_n|r^n)_{n\in\mathbf{N}}$ est bornée, resp. la suite $(|a_n|r^n)_{n\in\mathbf{N}}$ tend vers 0 quand n tend vers $+\infty$).

De même, on note $\mathscr{B}_K^{]r}$ (resp. $\mathscr{B}_K^{(r}$, resp. $\mathscr{B}_K^{[r}$) l'ensemble des séries de Laurent de la forme $\sum_{n\in\mathbf{Z}} a_n T^n$ à coefficients dans K telles que la suite de terme général $|a_n|\rho^n$ tend vers 0 quand n tend vers $-\infty$ quel que soit $\rho > r$ (resp. la suite $(|a_n|r^n)_{n\in-\mathbf{N}}$ est bornée, resp. la suite $(|a_n|r^n)_{n\in-\mathbf{N}}$ tend vers 0 quand n tend vers $-\infty$).

Si $r \leqslant s$ et $\langle$ (resp. $\rangle$) est l'un des symboles], (ou [(resp. [,) ou]), on pose $\mathscr{B}_K^{\langle r,s\rangle} = \mathscr{B}_K^{\langle r} \cap \mathscr{B}_K^{s\rangle}$. Si $r < s$, alors $\mathscr{B}_K^{\langle r,s\rangle}$ est une algèbre et si $r = s$, seuls $\mathscr{B}_K^{[r,r]}$, $\mathscr{B}_K^{[r,r)}$ et $\mathscr{B}_K^{(r,r]}$ sont munis d'une structure d'algèbre.

Exemple II.2. — i) $\mathscr{B}_K^{[0,1)}$ est l'algèbre des séries entières à coefficients bornés

ii) $\mathscr{B}_K^{[0,1[}$ est l'algèbre des séries entières de rayon de convergence 1.

iii) $\mathscr{B}_K^{[1,1)}$ est l'ensemble des séries de Laurent de la forme $\sum_{n\in\mathbf{Z}} a_n T^n$ dont les coefficients sont bornés et vérifient $\lim\limits_{n\to-\infty} a_n = 0$.

iv) Si $r \leqslant s$, alors $\mathscr{B}_K^{[r,s]}$ est l'algèbre des fonctions analytiques sur la couronne fermée $r \leqslant |T| \leqslant s$

v) Si $r < s$, alors $\mathscr{B}_K^{[r,s[}$ est l'algèbre des fonctions analytiques sur la couronne ouverte $r \leqslant |T| < s$ ouverte en s et fermée en r et $\mathscr{B}_K^{[r,s)}$ est la sous-algèbre de $\mathscr{B}_K^{[r,s[}$ des fonctions bornées au voisinage de $|T| = s$.

Lemme II.3. — *Si $r \leqslant s$, tout élément F de $\mathscr{B}_K^{[r,s]}$ s'écrit de manière unique sous la forme $F = PU$, où $P \in K[X]$ est un polynôme unitaire dont toutes les racines $\alpha \in \mathbf{C}_p$ vérifient $r \leqslant |\alpha| \leqslant s$ et U est inversible dans $\mathscr{B}_K^{[r,s]}$.*

ii) Si $r < s$, tout élément F de $\mathscr{B}_K^{[r,s)}$ s'écrit de manière unique sous la forme $F = PU$, où $P \in K[X]$ est un polynôme unitaire dont toutes les racines $\alpha \in \mathbf{C}_p$ vérifient $r \leqslant |\alpha| < s$ et U est inversible dans $\mathscr{B}_K^{[r,s)}$.

Démonstration. — C'est une conséquence de la théorie des polygones de Newton pour les séries de Laurent (cf. [**6**] par exemple)

Remarque II.4. — On a un énoncé analogue pour $\mathscr{B}_K^{(r,s)}$ mais pas pour $\mathscr{B}_K^{[r,s[}$ car un élément de $\mathscr{B}_K^{[r,s[}$ peut très bien avoir une infinité de zéros dans la couronne $r \leqslant |x| < s$ comme le montre l'exemple du logarithme.

La proposition suivante fait le lien entre ces anneaux de séries formelles et certains sous-anneaux de $\mathbf{B}_K$ ou $\mathbf{B}_{\mathrm{cris}}$ dont nous aurons besoin par la suite.

Proposition II.5. — *Si K est une extension non ramifiée de $\mathbf{Q}_p$, alors l'application qui à F associe $F(\pi)$ induit un isomorphisme*

i) de $\mathscr{B}_K^{[1,1)}$ sur $\mathbf{B}_K$,

ii) de $\mathscr{B}_K^{[0,1)}$ sur $\mathbf{B}_K^+$,

iii) de $\mathscr{B}_K^{[\rho_n,1)}$ sur $\mathbf{B}_K^{\dagger,n}$ si $n \geqslant 1$ et $\rho_n = |\varepsilon^{(n)} - 1| = p^{\frac{-1}{(p-1)p^{n-1}}}$,

iv) de $\mathscr{B}_K^{[0,1[}$ sur l'ensemble des transformées de Fourier des distributions continues sur $\mathbf{Z}_p$ à valeurs dans K.

Démonstration. — Le i) et le ii) sont des évidences, le iii) est démontré dans [**3**, Prop. II.2.1] et le iv) dans [**5**, Chap. VIII].

2. Les applications $\mathrm{Exp}^*_{V^*(1)}$ et Log_V.— Si K est une extension finie de $\mathbf{Q}_p$ et M est un $\mathscr{G}_K$-module topologique, on note $H^1(K,M)$ le premier groupe de cohomologie continue de $\mathscr{G}_K$ à coefficients dans M. Soit Λ_K l'algèbre de groupe complétée $\mathbf{Z}_p[[\Gamma_K]]$ de Γ_K qui peut aussi se voir comme l'algèbre des mesures sur Γ_K à valeurs dans $\mathbf{Z}_p$. Si V est une représentation p-adique de $\mathscr{G}_K$, on pose $H^1_{\mathrm{Iw}}(K,V) = H^1(K, \Lambda_K \otimes_{\mathbf{Z}_p} V)$. Rappelons que si T est un réseau de V stable par $\mathscr{G}_K$, le lemme de Shapiro nous fournit un isomorphisme canonique de $H^1_{\mathrm{Iw}}(K,V)$ sur $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \left(\varprojlim H^1(K_n,T)\right)$, la limite projective étant prise relativement aux applications de corestriction [**5**, Chap. II].

Le corps $\mathbf{B}$ est une extension de degré p de $\varphi(\mathbf{B})$, ce qui nous permet de définir un opérateur $\psi : \mathbf{B} \to \mathbf{B}$ par la formule $\psi(x) = p^{-1}\varphi^{-1}\big(\mathrm{Tr}_{\mathbf{B}/\varphi(\mathbf{B})}(x)\big)$. L'opérateur ψ commute à l'action de $\mathscr{G}_K$ et on a $\psi(\varphi(x)) = x$ si $x \in \mathbf{B}$ et $\psi(\mathbf{A}) \subset \mathbf{A}$. De manière explicite, $1, [\varepsilon], \dots, [\varepsilon]^{p-1}$ forment une base de $\mathbf{B}$ sur $\varphi(\mathbf{B})$ et on a $\psi(\sum_{i=0}^{p-1} a_i[\varepsilon]^i) = \varphi^{-1}(a_0)$ si $a_0, \dots, a_{p-1}$ sont des éléments de $\varphi(\mathbf{B})$.

Comme ψ commute à l'action de $\mathscr{G}_K$, si V est une représentation p-adique de $\mathscr{G}_K$, le module $D(V)$ hérite d'une action de ψ et le module $D(V)^{\psi=1}$ est très lié à la cohomologie galoisienne de V (cf. [**13**] et [**4**]). En particulier, il existe une application naturelle $\mathrm{Log}^*_{V^*(1)} : D(V)^{\psi=1} \to H^1_{\mathrm{Iw}}(K,V)$ et on a le résultat suivant :

Proposition II.6. — *Soient K une extension finie de $\mathbf{Q}_p$ et V une représentation p-adique de $\mathscr{G}_K$. Alors*

i) l'application $\mathrm{Log}^*_{V^*(1)} : D(V)^{\psi=1} \longrightarrow H^1_{\mathrm{Iw}}(K,V)$ est un isomorphisme (son inverse est noté $\mathrm{Exp}^*_{V^*(1)}$),

ii) il existe $n(V) \in \mathbf{N}$ tel que $D(V)^{\psi=1}$ soit inclus dans $D^{\dagger,n(V)}(V)$.

Démonstration. — Le i) [resp. le ii)] est démontré dans [**4**, Chap. II] (resp. [**4**, Chap. III]).

Si V est une représentation p-adique de $\mathscr{G}_K$, on note $H^1_e(K,V) \subset H^1(K,V)$ le noyau de l'application naturelle de $H^1(K,V)$ dans $H^1(K, \mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes V)$. On dit que V vérifie la condition $(*)$ si l'on a $H^1(L,V) = H^1_e(L,V)$ quelle que soit l'extension finie L de K. Si V est de de Rham, il existe $k_0 \in \mathbf{Z}$ tel que $V(k)$ vérifie la condition $(*)$ quel que soit $k \geqslant k_0$ car $H^1_e(L,V)$ est l'image de $L \otimes_K D_{\mathrm{dR}}(V)$ par l'exponentielle de Bloch-Kato [**2**] et celle-ci est un isomorphisme pour des raisons de dimensions, si on remplace V par $V(k)$ pour $k \gg 0$.

Soit T_n l'unique application $K_n((t))$-linéaire continue de $\mathbf{B}_{\mathrm{dR}}^{\mathscr{H}_K}$ dans $K_n((t))$ telle que si $m \geqslant n$ et $x \in K_m$, alors $\mathrm{T}_n(x) = p^{-m}\mathrm{Tr}_{K_m/K_n}(x)$ (cf. [**5**, Chap. V] pour la démonstration de l'existence et de l'unicité de cette application). Si V est de de Rham, l'application naturelle de $\mathbf{B}_{\mathrm{dR}}^{\mathscr{H}_K} \otimes_K D_{\mathrm{dR}}(V)$ dans $(\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{\mathscr{H}_K}$ est un isomorphisme, ce qui permet d'étendre les applications T_n pour $n \in \mathbf{N}$ par linéarité en des applications

$$\mathrm{T}_n : (\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{\mathscr{H}_K} \to K_n((t)) \otimes_K D_{\mathrm{dR}}(V).$$

Si V est une représentation de de Rham vérifiant la condition $(*)$, soit

$$\mathrm{Log}_V : H^1_{\mathrm{Iw}}(K,V) \to (\mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes_{\mathbf{Q}_p} V)^{\mathscr{H}_K}$$

l'application construite dans [**5**, Chap. VI]. La proposition suivante rassemble les propriétés de cette application que nous utiliserons dans la suite.

Proposition II.7. — *i) Si K est une extension finie de $\mathbf{Q}_p$ et V est une représentation de de Rham de $\mathscr{G}_K$ vérifiant la condition $(*)$, alors il existe $m(V) \geqslant n(V)$ tel que si $n \geqslant m(V)$ et $\mu \in H^1_{\mathrm{Iw}}(K,V)$,*

$$p^{-n}\varphi^{-n}(\mathrm{Exp}^*_{V^*(1)}(\mu)) = t\frac{d}{dt}(\mathrm{T}_n(\mathrm{Log}_V(\mu))).$$

ii) Si K est non ramifiée sur $\mathbf{Q}_p$, V est une représentation cristalline de $\mathscr{G}_K$ vérifiant la condition $(*)$ et $\mu \in H^1_{\mathrm{Iw}}(K,V)$, alors il existe une unique série $F_\mu(T) \in \mathscr{B}_K^{[0,1[} \otimes D_{\mathrm{cris}}(V)$, telle que l'on ait

$$\mathrm{T}_n(\mathrm{Log}_V(\mu)) = p^{-n}\varphi^{-n}(F_\mu(\pi)) \in K_n[[t]] \otimes D_{\mathrm{cris}}(V),$$

quel que soit $n \geqslant 1$.

Démonstration. — L'application Log_V est celle considérée dans [**4**] ; elle correspond à l'application $\mathrm{Log}_V^{(1)}$ de [**5**, Chap. VI] et le i) [resp. le ii)] est démontré dans [**4**, Th. IV.3.3] (resp. [**5**, Prop. IX.3.3]).

3. Point de départ de la démonstration

Proposition II.8. — *La matrice de φ dans une base $e_1, \dots, e_d$ de $D(V)$ constituée d'éléments de $D(V)^{\psi=1}$ appartient à $\mathrm{GL}_d(\mathrm{Fr}(\mathbf{B}_K^+))$.*

Démonstration. — Quitte à remplacer V par $V(k)$ pour $k \gg 0$, on peut supposer que V vérifie la condition $(*)$. Si $e_1, \dots, e_d$ est une base de $D(V)$ sur $\mathbf{B}_K$ constituée d'éléments de $D(V)^{\psi=1}$, alors d'après la proposition II.6, c'est aussi une base de $D^\dagger(V)$ sur $\mathbf{B}_K^\dagger$ et il existe une matrice $\Phi = (a_{i,j}) \in \mathrm{GL}_d(\mathbf{B}_K^\dagger)$ telle que l'on ait $\varphi(e_i) = \sum_{j=1}^d a_{i,j} e_j$. D'autre part, les $a_{i,j}$ sont éléments de $\mathbf{B}_K^\dagger$ et il existe donc $\rho \in [0,1[$ et des éléments $F_{i,j}$ de $\mathscr{B}_K^{[\rho,1)}$ tels que l'on ait $a_{i,j} = F_{i,j}(\pi)$. On note $F \in \mathrm{M}_d(\mathscr{B}_K^{[\rho,1)})$ la matrice de coefficients $F_{i,j}$.

Si $1 \leqslant j \leqslant d$, soit $\mu_j = \mathrm{Log}^*_{V^*(1)}(e_j) \in H^1_{\mathrm{Iw}}(K,V)$ et H_j l'unique élément de $\mathscr{B}_K^{[0,1[} \otimes \mathrm{D}_{\mathrm{cris}}(V)$ telle que l'on ait $p^n \mathrm{T}_n(\mathrm{Log}_V(\mu_j)) = \varphi^{-n}(H_j(\pi))$ si $n \geqslant 1$. Soit

$$G_j = \log(1+T)(1+T)\frac{d}{dT}H_j \in \mathscr{B}_K^{[0,1[} \otimes \mathrm{D}_{\mathrm{cris}}(V)$$

de telle sorte que l'on a $G_j(\pi) = t\frac{d}{dt}H_j(\pi)$ car $t = \log(1+\pi)$. Il résulte du i) de la proposition II.7 et du fait que $t\frac{d}{dt}$ commute à φ, qu'il existe $m(V) \in \mathbf{N}$ tel que l'on ait

$$\varphi^{-m}(e_j) = \varphi^{-m}(G_j(\pi)) \quad \text{si} \quad m \geqslant m(V). \tag{II.9}$$

Soit $f_1, \ldots, f_d$ une base de $\mathrm{D}_{\mathrm{cris}}(V)$ sur K. On peut décomposer G_j sous la forme $\sum_{k=1}^d G_{j,k} f_k$ dans la base $f_1, \ldots, f_d$ et appliquer φ^{-m} à l'identité $\varphi(e_i) = \sum_{j=1}^d F_{i,j}(\pi) e_j$ si $m > m(V)$. On obtient, en utilisant la relation (II.9)

$$\sum_{l=1}^d G_{i,l}^{\varphi^{1-m}}(\pi_{m-1})\varphi^{1-m}(f_l) = \sum_{j=1}^d F_{i,j}^{\varphi^{-m}}(\pi_m)\Big(\sum_{k=1}^d G_{j,k}^{\varphi^{-m}}(\pi_m)\varphi^{-m}(f_k)\Big),$$

où, si $m \in \mathbf{N}$, on a posé $\pi_m = \varphi^{-m}(\pi)$ et, si H appartient à $\mathscr{B}_K^{\langle r,s\rangle}$ ou à $\mathscr{B}_K^{\langle r,s\rangle} \otimes \mathrm{D}_{\mathrm{cris}}(V)$, on a noté $H^{\varphi^{-m}}$ la série dont les coefficients sont ceux de H auxquels on a appliqué φ^{-m}. Compte-tenu du fait que $\mathscr{B}_K^{[\rho_m,1)}$ et $\mathscr{B}_K^{[0,1[}$ sont inclus dans $\mathscr{B}_K^{[\rho_m,\rho_m]}$ et que l'application de $\mathscr{B}_K^{[\rho_m,\rho_m]}$ dans $\mathbf{B}^+_{\mathrm{dR}}$ qui à F associe $F(\pi_m)$ est injective (cf. §5), ceci nous fournit l'égalité matricielle

$$G^{\varphi}((1+T)^p - 1)M^{\varphi} = F(T)G(T), \tag{II.10}$$

où $M = (m_{i,j})_{1\leqslant i,j\leqslant d} \in \mathrm{GL}_d(K)$ est la matrice définie par $\varphi(f_i) = \sum_{i=1}^d m_{i,j} f_j$ et $G \in \mathrm{M}_d(\mathscr{B}_K^{[0,1[})$ est la matrice dont le coefficient de la j-ième ligne et la k-ième colonne est $G_{j,k}$.

Lemme II.11. — $\det G \neq 0$.

Démonstration. — Soit $v_1, \ldots, v_d$ une base de V sur $\mathbf{Q}_p$. Par hypothèse, $e_1, \ldots, e_d$ forment une base de $D(V)$ sur $\mathbf{B}_K$ et donc aussi de $\mathbf{B} \otimes_{\mathbf{Q}_p} V = \mathbf{B} \otimes_{\mathbf{B}_K} D(V)$ sur $\mathbf{B}$. Ceci implique que le déterminant de $e_1, \ldots, e_d$ dans la base $e_1, \ldots, e_d$ est non nul et donc aussi que le déterminant de $\varphi^{-n}(e_1), \ldots, \varphi^{-n}(e_d)$ dans la base des $\varphi^{-n}(v_i) = v_i$ est non nul. Or ce dernier déterminant est aussi égal à $\det(G^{\varphi^{-n}}(\pi_n)) \det_{v_1,\ldots,v_n}(\varphi^{-n}(f_1), \ldots, \varphi^{-n}(f_d))$, ce qui permet de conclure.

On déduit de ce lemme et de l'identité (II.10) ci-dessus le fait que $F(T)$ est à coefficients dans $\mathrm{Fr}(\mathscr{B}_K^{[0,1[})$ et comme elle est aussi à coefficients dans $\mathscr{B}_K^{[\rho,1)}$. Pour conclure la démonstration de la proposition II.8, il suffit alors d'utiliser le lemme suivant et le ii) de la proposition II.5.

Lemme II.12. — *Si $0 \leqslant \rho < 1$, alors $\mathscr{B}_K^{[\rho,1)} \cap \mathrm{Fr}(\mathscr{B}_K^{[0,1[}) \subset \mathrm{Fr}(\mathscr{B}_K^{[0,1)})$.*

Démonstration. — Soit F appartenant à l'intersection. On peut donc écrire F sous la forme $\frac{G}{H}$ avec $G, H \in \mathscr{B}_K^{[0,1[}$. Soit $\eta \in]\rho, 1[$. Il existe un (unique) polynôme P unitaire dont toutes les racines vérifient $|\alpha| \leqslant \eta$ et U inversible dans $\mathscr{B}_K^{[0,\eta]}$ tels que l'on ait $H = PU$. On en déduit le fait que $PF \in \mathscr{B}_K^{[0,\eta]}$ et comme d'autre part, $PF \in \mathscr{B}_K^{[\rho,1)}$ et $\rho < \eta$, ceci implique $PF \in \mathscr{B}_K^{[0,1)}$ et permet de conclure.

Lemme II.13. — *Si $e_1,\dots,e_d$ est une base de $D(V)$ sur $\mathbf{B}_K$ constituée d'éléments de $D(V)^{\psi=1}$ tels que les familles $((\gamma-1)e_i)_{1\leqslant i\leqslant d}$ et $((\varphi-1)(\gamma-1)e_i)_{1\leqslant i\leqslant d}$ soient des bases de $D(V)$ sur $\mathbf{B}_K$, alors la matrice de γ dans la base $e_1,\dots,e_d$ appartient à $\mathrm{GL}_d(\mathrm{Fr}(\mathbf{B}_K^+))$.*

Démonstration. — Si $1\leqslant i\leqslant d$, posons $u_i=(\gamma-1)e_i$. Par hypothèse, $u_1,\dots,u_d$ forment une base de $D(V)$ qui est constituée d'éléments de $D(V)^{\psi=1}$ puisque ce module est stable par Γ et qu'il contient les e_i. Soient $A=(a_{i,j})$, $B=(b_{i,j})$ et $C=(c_{i,j})$ les éléments de $\mathrm{GL}_d(\mathbf{B}_K)$ définis par

$$\varphi(e_j)=\sum_{i=1}^d a_{i,j}e_i,\quad \gamma(e_j)=\sum_{i=1}^d b_{i,j}e_i\quad\text{et}\quad \varphi(u_j)=\sum_{i=1}^d c_{i,j}u_i,\ \text{si } 1\leqslant j\leqslant d.$$

D'après le lemme II.8, A et C appartiennent à $\mathrm{GL}_d(\mathrm{Fr}(\mathbf{B}_K^+))$ et notre problème est de montrer qu'il en est de même de B. Par construction, on a d'une part $\varphi(u_k)=\sum_{j=1}^d c_{j,k}u_j$ et d'autre part, comme φ et γ commutent

$$\varphi(u_k)=\varphi((\gamma-1)e_k)=(\gamma-1)(\sum_{j=1}^d a_{j,k}e_k)=\sum_{j=1}^k(\gamma-1)a_{j,k}e_j+\sum_{j=1}^k\gamma(a_{j,k})u_j.$$

On en tire l'égalité

$$\sum_{j=1}^d(c_{j,k}-\gamma(a_{j,k}))u_j=\sum_{i=1}^d(\gamma-1)a_{i,k}e_i$$

qui se traduit matriciellement par

$$(B-1)(C-\gamma(A))=\gamma(A)-1\quad\text{ou encore}\quad B(C-\gamma(A))=C-1.$$

Comme on a supposé que $(u_i)_{1\leqslant i\leqslant d}$ et $((\varphi-1)u_i)_{1\leqslant i\leqslant d}$ sont des bases de $D(V)$ sur $\mathbf{B}_K$, cela implique que $C-1$ qui est la matrice des $(\varphi-1)u_i$ dans la base des u_i, est inversible et donc que B aussi, ce qu'il fallait démontrer.

4. Construction de bases de $D(V)$.— Pour terminer la démonstration de la proposition II.1, il s'agit de montrer que l'on peut trouver des bases de $D(V)$ satisfaisant les conditions des lemmes II.8 et II.13 ; autrement dit, il s'agit de démontrer la proposition (technique) suivante.

Proposition II.14. — *Si V est une représentation p-adique de $\mathscr{G}_K$, il existe $n\in\mathbf{N}$ et une base $e_1,\dots,e_d$ de $D(V)$ sur $\mathbf{B}_K$ constitué d'éléments de $D(V)^{\psi=1}$ tels que les familles $((\sigma-1)e_i)_{1\leqslant i\leqslant d}$ et $((\varphi-1)(\sigma-1)e_i)_{1\leqslant i\leqslant d}$ soient des bases de $D(V)$ sur $\mathbf{B}_K$ quel que soit $\sigma\in\Gamma_{K_n}-\{1\}$.*

Démonstration. — Soient T un $\mathbf{Z}_p$-réseau de V stable par $\mathscr{G}_K$ et $\overline{T}=T/pT$. L'un des ingrédients essentiels pour démontrer la proposition ci-dessus est que l'image M de $D(T)^{\psi=1}$ dans $D(\overline{T})^{\psi=1}$ est un sous-$\mathbf{F}_p$-espace vectoriel de codimension finie de $D(\overline{T})^{\psi=1}$ (cf. [**4**] démonstration du corollaire I.7.6). Soit r cette codimension.

Si $n\geqslant 2$, soit γ_n un générateur topologique de Γ_{K_n}. Soit $f_1,\dots,f_d$ une base de $N=(\mathfrak{m}_{\mathbf{E}}\otimes\overline{T})^{\mathscr{H}_K}$ sur $\mathbf{E}_K^+$ et choisissons un entier $n\geqslant 2$ tel que la matrice de γ_n dans la base $f_1,\dots,f_d$ appartienne à $1+\pi\mathrm{M}_d(\mathbf{E}_K^+)$. Soit $k\in\mathbf{N}$ tel que $p^k\geqslant p^n+p(r+1)$ et, si $1\leqslant i\leqslant d$, soit $g_i=\varphi^k(f_i)$. La matrice de γ_n dans la base $g_1,\dots,g_d$ appartient donc à $1+\varphi^k(\pi)\mathrm{M}_d(\mathbf{E}_K^+)\subset 1+\pi^{p^n+p(r+1)}\mathrm{M}_d(\mathbf{E}_K^+)$. Soit $N'=\varphi^k(N)$ le sous-$\mathbf{E}_K^+$-module de $D(\overline{T})$ engendré par $g_1,\dots,g_d$. Il est stable par φ. Soit eul : $(\mathfrak{m}_{\mathbf{E}}^{\psi=0}\otimes\overline{T})^{\mathscr{H}_K}\to D(\overline{T})^{\psi=1}$ l'application définie par $\mathrm{eul}(x)=\sum_{n=0}^{+\infty}\varphi^n(x)$.

Lemme II.15. — *Si $1 \leqslant i \leqslant d$, il existe $\beta_i \in \varepsilon\varphi(\mathbf{E}_K)$ vérifiant $2p(r+1) \leqslant v_{\mathbf{E}}(\beta_i) < 3p(r+1)$ tel que $h_i = \mathrm{eul}(\beta_i g_i)$ appartienne à M.*

Démonstration. — Si $j \in \mathbf{N}$, soit $z_j = \mathrm{eul}(\varepsilon\pi^{2p(r+1)+pj} g_i)$. Les z_j pour $0 \leqslant j \leqslant r$ forment une famille de $r+1$ éléments de $D(\overline{T})^{\psi=1}$ et comme M est de codimension r dans $D(\overline{T})^{\psi=1}$, il existe des $a_j \in \mathbf{F}_p$ pour $0 \leqslant j \leqslant r$ non tous nuls tels que $\sum_{j=0}^r a_j z_j \in M$. On peut alors prendre $\beta_i = \varepsilon\pi^{2p(r+1)} \sum_{j=0}^r a_j \pi^{pj}$.

Munissons $D(\overline{T})$ de la valuation $v_{\mathbf{E}}$ définie en prenant le $\mathbf{E}_K^+$-réseau N' de $D(\overline{T})$ engendré par $\varphi^k(N)$ comme réseau des éléments entiers. Autrement dit, $v_{\mathbf{E}}$ est définie par la formule $v_{\mathbf{E}}(x) = m$ si $x \in \pi^m N' - \pi^{m+1} N'$.

Lemme II.16. — *Si $\sigma \in \Gamma_{K_n} - \{1\}$, soit $v(\sigma) = v_p(\chi(\sigma) - 1)$.*
i) Si $a \in \mathbf{N}$, $\sigma \in \Gamma_{K_n}$ et $x \in \pi^{pa}\mathbf{E}_K^+$, alors $v_{\mathbf{E}}((\sigma-1)x) \geqslant pa + p^{v(\sigma)}$
ii) Si $x \in \varepsilon\varphi(\mathbf{E}_K^+)$, alors $v_{\mathbf{E}}((\sigma-1)x) = v_{\mathbf{E}}(x) + p^{v(\sigma)}$
iii) Si $\sigma \in \Gamma_{K_n} - \{1\}$ et $1 \leqslant i \leqslant d$, alors $v_{\mathbf{E}}((\sigma-1)g_i) \geqslant p^{v(\sigma)} + p(r+1)$.

Démonstration. — i) Si $a = 0$, il s'agit de prouver que si $x \in \mathbf{E}_K^+$, alors $v_{\mathbf{E}}(\sigma(x) - x) \geqslant p^{v(\sigma)}$. Il suffit de vérifier cette inégalité pour les polynômes en ε puisque ceux-ci sont denses dans $\mathbf{E}_K^+$ et le résultat découle de l'identité

$$\sigma(\varepsilon^i) - \varepsilon^i = \varepsilon^i(\varepsilon^{i(\chi(\sigma)-1)} - 1) = \varepsilon^i\big(\varepsilon^{i\frac{\chi(\sigma)-1}{p^{v(\sigma)}}} - 1\big)^{p^{v(\sigma)}}.$$

Le cas général se démontre par récurrence sur a en utilisant l'identité

$$(\sigma - 1)(\pi^p x) = \sigma(\pi^p)(\sigma(x) - x) + (\sigma(\pi) - \pi)^p x$$

qui nous fournit l'inégalité

$$v_{\mathbf{E}}((\sigma-1)(\pi^p x)) \geqslant \inf\big(p + v_{\mathbf{E}}(\sigma(x) - x), p^{v(\sigma)+1} + v_{\mathbf{E}}(x)\big).$$

ii) On part de la formule $(\sigma-1)(\varepsilon\varphi(y)) = (\sigma(\varepsilon)-\varepsilon)\varphi(y) + \sigma(\varepsilon)\varphi(\sigma(y)-y)$ et comme, d'après le i), on a

$$v_{\mathbf{E}}(\varphi(\sigma(y)-y)) = pv_{\mathbf{E}}(\sigma(y)-y) \geqslant p\Big(p^{v(\sigma)} + p[\frac{v_{\mathbf{E}}(y)}{p}]\Big) > v_{\mathbf{E}}(\varphi(y)) + p^{v(\sigma)},$$

on en déduit le résultat en écrivant $x \in \varepsilon\varphi(\mathbf{E}_K^+)$ sous la forme $\varepsilon\varphi(y)$.

iii) La démonstration se fait par récurrence sur $v(\sigma)$. Si $v(\sigma) \geqslant n$, alors $\frac{\sigma-1}{\gamma_n-1} \in \mathbf{Z}_p[[\Gamma]]$ et comme N' est stable par Γ, on a $v_{\mathbf{E}}((\sigma-1)g_i) \geqslant v_{\mathbf{E}}((\gamma_n-1)g_i) \geqslant p^n + p(r+1)$, ce qui démontre l'inégalité voulue si $v(\sigma) = n$. Si $v(\sigma) \geqslant n+1$, on peut écrire σ sous la forme τ^p avec $v(\tau) = v(\sigma) - 1 \geqslant n$ et on a $(\sigma-1)g_i = (\tau^p-1)g_i = (\tau-1)^p g_i = (\tau-1)^{p-1}((\tau-1)g_i)$. Par hypothèse, on a $v_{\mathbf{E}}((\tau-1)g_i) \geqslant p^{v(\tau)} + p(r+1)$ et une petite récurrence utilisant le i) et la formule $(\tau-1)(\sum_{i=1}^d \alpha_i g_i) = \sum_{i=1}^d (\tau(\alpha_i) - \alpha_i) g_i + \sum_{i=1}^d \tau(\alpha_i)(\tau(g_i) - g_i)$, permet de montrer que si $x \in N'$ vérifie $v_{\mathbf{E}}(x) \geqslant pa$, alors $v_{\mathbf{E}}((\tau-1)^j x) \geqslant pa + jp^{v(\tau)}$. On en déduit le résultat.

Lemme II.17. — *i) $v_{\mathbf{E}}(h_i - \beta_i g_i) \geqslant 2p^2(r+1)$*
Si $\sigma \in \Gamma_n - \{1\}$, soit $\beta_{i,\sigma} = (\sigma-1)\beta_i$, alors
ii) $v_{\mathbf{E}}((\sigma-1)h_i - \beta_{i,\sigma} g_i) \geqslant p^{v(\sigma)} + 3p(r+1)$.
iii) $v_{\mathbf{E}}((\varphi-1)(\sigma-1)h_i - \beta_{i,\sigma} g_i) \geqslant p^{v(\sigma)} + 3p(r+1)$.

Démonstration. — Comme $\varphi^k(N)$ est stable par φ puisque N l'est, la formule $\mathrm{eul}(x) = x + \varphi(x) + \cdots$ montre que si $v_{\mathbf{E}}(x) \geqslant 0$, alors $v_{\mathbf{E}}(\mathrm{eul}(x) - x) \geqslant pv_{\mathbf{E}}(x)$, ce qui permet de prouver le i) car $v_{\mathbf{E}}(h_i) = v_{\mathbf{E}}(\beta_i) \geqslant 2p(r+1)$. Le ii) se déduit du iii) de la même manière. Finalement, comme

$$(\varphi - 1)(\sigma - 1)h_i = (\sigma - 1)(\varphi - 1)h_i = (\sigma - 1)(\beta_i g_i) = \beta_{i,\sigma} g_i + \sigma(\beta_i)(\sigma(g_i) - g_i),$$

on déduit le iii) du lemme iii) du lemme II.16.

Corollaire II.18. — *La famille $(h_i)_{1 \leqslant i \leqslant d}$ et, si $\sigma \in \Gamma_n - \{1\}$, les familles $((\sigma - 1)h_i)_{1 \leqslant i \leqslant d}$ et $((\varphi - 1)(\sigma - 1)h_i)_{1 \leqslant i \leqslant d}$ forment des bases de $D(\overline{T})$ sur $\mathbf{E}_K$.*

Démonstration. — Comme $g_1, \ldots, g_d$ forment une base de $\varphi^k(N)$ sur $\mathbf{E}_K^+$, le fait que $h_1, \ldots, h_d$ forment une base de $D(\overline{T})$ sur $\mathbf{E}_K$ est une conséquence du i) du lemme précédent et de la majoration $v_{\mathbf{E}}(\beta_i) < 3p(r+1) \leqslant 2p^2(r+1)$. De même, le reste du corollaire s'obtient en utilisant les ii) et iii) du lemme II.17 et la majoration $v_{\mathbf{E}}(\beta_{i,\sigma}) < p^{v(\sigma)} + 3p(r+1)$ que l'on déduit du ii) du lemme II.16.

Pour construire une base de $D(V)$ satisfaisant les propriétés de la proposition II.14, il suffit alors de prendre pour e_i un relèvement quelconque de h_i dans $D(T)^{\psi=1}$ (c'est possible car on a pris la précaution de prendre les h_i dans M).

5. Convergence de séries dans $\mathbf{B}_{\mathrm{dR}}^+$.— Ce paragraphe est consacré à la démonstration de la proposition suivante qui a été utilisée au cours de la démonstration du lemme II.8.

Proposition II.19. — *Soient $x \in \mathbf{B}_{\mathrm{dR}}^+$ transcendant sur $\mathbf{Q}_p$ et $\rho = |\theta(x)|$.*

i) Si $F = \sum_{n \in \mathbf{Z}} a_n T^n \in \mathscr{B}_K^{[\rho,\rho]}$, la série $\sum_{n \in \mathbf{Z}} a_n x^n$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$ vers une limite notée $F(x)$.

ii) L'application qui à $F \in \mathscr{B}_K^{[\rho,\rho]}$ associe $F(x)$ est un morphisme injectif d'algèbres de $\mathscr{B}_K^{[\rho,\rho]}$ dans $\mathbf{B}_{\mathrm{dR}}^+$.

Démonstration. — Si on admet le i), le fait que $F \to F(x)$ soit un morphisme d'algèbre est une évidence et l'injectivité de ce morphisme vient de ce que tout idéal de $\mathscr{B}_K^{[\rho,\rho]}$ est engendré par un polynôme et de ce que l'on a supposé x transcendant sur $\mathbf{Q}_p$. Il n'y a donc que le i) à prouver ce qui va nécessiter un peu de préparation.

Lemme II.20. — *Si E est un sous-ensemble de $\mathbf{B}_{\mathrm{dR}}^+$, les propriétés suivantes sont équivalentes.*

(i) Quelle que soit la suite x_m d'éléments de E et quelle que soit la suite y_m d'éléments de $\mathbf{B}_{\mathrm{dR}}^+$ tendant vers 0, la suite $x_m y_m$ tend vers 0.

(ii) Quelle que soit la suite x_m d'éléments de E, la suite $p^m x_m$ tend vers 0.

(iii) Quel que soit $k \in \mathbf{N}$, il existe $n_k \in \mathbf{N}$ tel que $E \subset p^{-n_k}\widetilde{\mathbf{A}}^+ + (\ker \theta)^{k+1}$.

Démonstration. — (i)⇒(ii) de manière immédiate. Supposons que la propriété (iii) ne soit pas vérifiée ; il existe alors $k \in \mathbf{N}$ tel que pour tout $n \in \mathbf{N}$, on puisse trouver $x_m \in E$ n'appartenant pas à $p^{-m}\widetilde{\mathbf{A}}^+ + (\ker \theta)^{k+1}$. Mais alors la suite $p^m x_m$ n'a aucun terme dans $\widetilde{\mathbf{A}}^+ + (\ker \theta)^{k+1}$ et comme ce dernier ensemble est un voisinage de 0, on en tire le fait que la suite $p^m x_m$ ne tend pas vers 0 et donc que la propriété (ii) n'est pas vérifiée non plus. Il reste à montrer (iii)⇒(i). Soit y_m une suite d'éléments de $\mathbf{B}_{\mathrm{dR}}^+$ tendant vers 0. Par définition de la topologie de

$\mathbf{B}_{\mathrm{dR}}^+$, ceci est équivalent au fait que, quel que soit $k\in\mathbf{N}$, il existe $N_{k,n}\in\mathbf{N}$ tel que l'on ait $y_m\in p^n\widetilde{\mathbf{A}}^+ + (\ker\theta)^{k+1}$ si $m\geqslant N_{k,n}$. Mais alors, si x_m est une suite d'éléments de E, on a $x_my_m\in p^n\widetilde{\mathbf{A}}^+ + (\ker\theta)^{k+1}$ si $m\geqslant N_{k,n+n_k}$, ce qui montre que la suite x_my_m tend vers 0 et termine la démonstration du lemme.

Définition II.21. — *Un sous-ensemble E de $\mathbf{B}_{\mathrm{dR}}^+$ vérifiant une des 3 propriétés équivalentes du lemme II.20 sera dit borné dans $\mathbf{B}_{\mathrm{dR}}^+$.*

Lemme II.22. — *(i) Un ensemble fini est borné.*

(ii) Si E_1 et E_2 sont bornés, les ensembles $E_1\cup E_2$, $E_1+E_2=\{x+y\mid x\in E_1 \text{ et } y\in E_2\}$ et $E_1.E_2=\{xy\mid x\in E_1 \text{ et } y\in E_2\}$ sont bornés.

(iii) Si E est borné le sous-$\mathbf{Z}_p$-module de $\mathbf{B}_{\mathrm{dR}}^+$ engendré par E est borné et l'adhérence du sous-groupe additif de $\mathbf{B}_{\mathrm{dR}}^+$ engendré par E est bornée dans $\mathbf{B}_{\mathrm{dR}}^+$.

(iv) Si E est un sous-ensemble de $\ker\theta$ borné dans $\mathbf{B}_{\mathrm{dR}}^+$ et $f\in\mathbf{B}_{\mathrm{dR}}^+[[X]]$, alors $f(E)$ est borné dans $\mathbf{B}_{\mathrm{dR}}^+$

Démonstration. — Le (i) est évident et les points (ii) et (iii) découlent du lemme II.20. Finalement, si E est un sous-ensemble borné de $(\ker\theta)$, son image par f modulo $(\ker\theta)^{k+1}$ est la même que celle par le polynôme obtenu en ne gardant que les termes de degré $\leqslant k$ dans le développement en série entière de f ; elle est donc bornée en vertu du (ii).

Lemme II.23. — *Soit E un sous-ensemble de $1+\ker\theta$ borné dans $\mathbf{B}_{\mathrm{dR}}^+$. Alors le sous-groupe de $(\mathbf{B}_{\mathrm{dR}}^+)^*$ engendré par E est borné dans $\mathbf{B}_{\mathrm{dR}}^+$.*

Démonstration. — On se ramène au (iii) du lemme II.22 via le (iv) de ce lemme appliqué aux applications log et exp qui induisent des isomorphismes analytiques de groupes entre $1+\ker\theta$ et $(\ker\theta)$.

Lemme II.24. — *Soit E un sous-ensemble borné de $\mathbf{B}_{\mathrm{dR}}^+$ inclus dans le sous-groupe $(\mathbf{B}_{\mathrm{dR}}^+)^{**}$ de $(\mathbf{B}_{\mathrm{dR}}^+)^*$ des éléments x vérifiant $|\theta(x)|=1$. Alors le sous-groupe de $(\mathbf{B}_{\mathrm{dR}}^+)^*$ engendré par E est borné dans $\mathbf{B}_{\mathrm{dR}}^+$.*

Démonstration. — Comme $\widetilde{\mathbf{A}}^+$ est borné, $E'=(1+\ker\theta)\bigcap\{xy^{-1}\mid x\in E, y\in(\widetilde{\mathbf{A}}^+)^*\}$ est un sous-ensemble de $1+\ker\theta$ borné dans $\mathbf{B}_{\mathrm{dR}}^+$ et E est inclus dans $(\widetilde{\mathbf{A}}^+)^*\cdot E'$ car θ induit une surjection de $(\widetilde{\mathbf{A}}^+)^*$ sur $\mathscr{O}_{\mathbf{C}_p}^*$ et E est donc borné.

Revenons à la démonstration de la proposition II.19. Soient $c\in\mathbf{N}-\{0\}$ et $d\in\mathbf{Z}$ tels que $|\theta(x)|^c=p^{-d}$. Tout élément n de $\mathbf{Z}$ s'écrit de manière unique sous la forme $n=cm+r$ avec $m\in\mathbf{Z}$ et $0\leqslant r\leqslant c-1$ et on pose $b_{r,m}=p^{md}a_{cm+r}$ si $m\in\mathbf{Z}$ et $0\leqslant r\leqslant c-1$. L'hypothèse selon laquelle $F\in\mathscr{B}_K^{[\rho,\rho]}$ est équivalente au fait que si $0\leqslant r\leqslant c-1$, la suite de terme général $b_{r,m}$ tend vers 0 quand $|m|$ tend vers $+\infty$ et on peut écrire $F(x)$ sous la forme

$$F(x)=\sum_{r=0}^{c-1}x^r\sum_{m\in\mathbf{Z}}b_{r,m}(p^{-d}x^c)^m,$$

série qui converge car l'ensemble des $(p^{-d}x^c)^m$ pour $m\in\mathbf{Z}$ est borné en vertu du lemme II.24 appliqué à $E=\{p^{-d}x^c\}$. Ceci termine la démonstration du i) de la proposition II.19.

Proposition II.25. — *Une série* $\sum_{k\gg-\infty} p^k[x_k]$*, où* $(x_k)_{k\in\mathbf{N}}$ *est une suite d'éléments de* $\widetilde{\mathbf{E}}$*, converge dans* $\mathbf{B}_{\mathrm{dR}}^+$ *si et seulement si* $\sum_{k\gg-\infty} p^k x_k^{(0)}$ *converge dans* $\mathbf{C}_p$*.*

Démonstration. — Si $\sum_{k\gg-\infty} p^k[x_k]$ converge dans $\mathbf{B}_{\mathrm{dR}}^+$, alors $\sum_{k\gg-\infty} p^k\theta([x_k]) = \sum_{k\gg-\infty} p^k x_k^{(0)}$ converge dans $\mathbf{C}_p$. Réciproquement, si $\sum_{k\gg-\infty} p^k x_k^{(0)}$ converge dans $\mathbf{C}_p$ et si a_k désigne la partie entière de $v_{\mathbf{E}}(x_k)$, alors $k+a_k$ tend vers $+\infty$ quand k tend vers $+\infty$. Si $\tilde{p}\in\widetilde{\mathbf{E}}^+$ vérifie $\tilde{p}^{(0)}=p$, on peut alors écrire $p^k[x_k]$ sous la forme $p^{k+a_k}u_k(p^{-1}[\tilde{p}])^{a_k}$ avec $u_k\in\widetilde{\mathbf{A}}^+$ et le lemme II.23 appliqué à $E=\{p^{-1}[\tilde{p}]\}$ implique que la suite de terme général $(p^{-1}[\tilde{p}])^{a_k}$ est bornée et donc que celle de terme général $p^k[x_k]$ tend vers 0 dans $\mathbf{B}_{\mathrm{dR}}^+$, ce qui permet de conclure.

III. Représentations de hauteur finie et (φ,Γ_K)-modules presque de hauteur finie.

Dans tout ce chapitre, on suppose que K est une extension finie non ramifiée de $\mathbf{Q}_p$, ce qui fait d'ailleurs que Γ_K est isomorphe à $\mathbf{Z}_p^*$.

1. Définitions et résultats.— Pour terminer la démonstration du théorème I.4, nous sommes amenés à étudier de plus près les (φ,Γ_K)-modules associés aux représentations de hauteur finie. Pour cela, nous allons introduire la terminologie suivante (heureusement provisoire comme le montre la proposition III.2).

Définition III.1. — *Un* (φ,Γ_K)*-module étale* D *de rang* d *sur* $\mathbf{B}_K$ *est dit être*

i) de hauteur finie s'il existe une base $e_1,\dots,e_d$ *de* D *sur* $\mathbf{B}_K$ *telle que le sous-*$\mathbf{B}_K^+$*-module de* D *engendré par* $e_1,\dots,e_d$ *soit stable par* φ*,*

ii) essentiellement de hauteur finie s'il existe un sous-groupe ouvert Γ *de* Γ_K *et une base* $e_1,\dots,e_d$ *de* D *sur* $\mathbf{B}_K$ *tels que le sous-*$\mathrm{Fr}(\mathbf{B}_K^+)$*-espace vectoriel engendré par* $e_1,\dots,e_d$ *soit stable par* φ *et le* $\mathbf{B}_K^+$*-module engendré par* $e_1,\dots,e_d$ *soit stable par* Γ*,*

iii) presque de hauteur finie s'il existe un sous-groupe ouvert Γ *de* Γ_K *et une base* $e_1,\dots,e_d$ *de* D *sur* $\mathbf{B}_K$ *tels que le sous-*$\mathrm{Fr}(\mathbf{B}_K^+)$*-espace vectoriel engendré par* $e_1,\dots,e_d$ *soit stable par* φ *et* Γ*.*

Au cours du chapitre II, nous avons démontré (proposition II.1) que si V est une représentation p-adique cristalline de $\mathscr{G}_K$, alors son (φ,Γ_K)-module est presque de hauteur finie. Le fait que V est de hauteur finie est donc une conséquence de la proposition suivante.

Proposition III.2. — *Si* V *est une représentation* p*-adique de* $\mathscr{G}_K$*, les conditions suivantes sont équivalentes :*

i) V *est de hauteur finie.*

ii) $D(V)$ *est de hauteur finie.*

iii) $D(V)$ *est essentiellement de hauteur finie.*

iv) $D(V)$ *est presque de hauteur finie.*

2. Représentations de hauteur finie et (φ,Γ)-modules de hauteur finie.— Dans ce paragraphe, nous allons démontrer l'équivalence des conditions i) et ii) de la proposition III.2. Il s'agit d'un résultat de Fontaine [**10**]. Nous aurons besoin du lemme suivant.

Lemme III.3. — *Si V est une représentation p-adique de $\mathscr{G}_K$ de dimension d sur $\mathbf{Q}_p$, alors $D^+(V)$ est un $\mathbf{B}_K^+$-module libre de rang inférieur ou égal à d.*

Démonstration. — Soient T un $\mathbf{Z}_p$-réseau de V stable par $\mathscr{G}_K$ et $\overline{T} = T/pT$. On a $D^+(V) = \mathbf{Q}_p \otimes D^+(T)$ et il suffit donc de prouver que $D^+(T)$ est un A_K^+-module libre de rang inférieur ou égal à d pour prouver le i). D'autre part, le $\mathbf{E}_K^+$-module $D^+(\overline{T})$ est un $\mathbf{E}_K^+$-réseau du $\mathbf{E}_K$-espace vectoriel $D(\overline{T})$; il est donc libre de rang d sur $\mathbf{E}_K^+$.

Soit N le sous-$\mathbf{E}_K^+$-module de $D(\overline{T})$ engendré par l'image de $D^+(T)$. C'est un sous-$\mathbf{E}_K^+$-module de $D^+(\overline{T})$ et, $\mathbf{E}_K^+$ étant principal, il est libre de rang $r \leqslant d$ sur $\mathbf{E}_K^+$. Soit $e_1, \ldots, e_r$ une famille d'éléments de $D^+(T)$ dont les images modulo p forment une base de N sur $\mathbf{E}_K^+$. Pour terminer la démonstration du i), il suffit de prouver que $e_1, \ldots, e_r$ forment une base de $D^+(T)$ sur $\mathbf{A}_K^+$ ou, de manière équivalente, que l'application qui à $x_1, \ldots, x_r \in \mathbf{A}_K^+$ associe $x_1e_1 + \cdots + x_re_r \in D^+(T)$ est un isomorphisme. Comme $(\mathbf{A}_K^+)^r$ et $D^+(T)$ sont séparés et complets pour la topologie p-adique, il suffit de vérifier ceci modulo p et l'injectivité est une conséquence du fait que l'on a $pD^+(T) = D^+(T) \cap pD(T)$ car $p\mathbf{A} \cap \mathbf{A}^+ = p\mathbf{A}^+$ et la surjectivité découle du fait que la réduction modulo p induit une surjection de $\mathbf{A}_K^+$ sur $\mathbf{E}_K^+$ puisque l'on a supposé K non ramifié sur $\mathbf{Q}_p$.

Corollaire III.4. — *Si V est de hauteur finie, alors $D(V)$ est de hauteur finie et essentiellement de hauteur finie.*

Démonstration. — Si V est de hauteur finie, $D^+(V)$ contient une base de $D(V)$ sur $\mathbf{B}_K$ et donc la dimension de $D^+(V)$ sur $\mathbf{B}_K^+$ est au moins égale à $\dim_{\mathbf{Q}_p} V$ et le lemme montre que l'on a égalité. Comme d'autre part, $D^+(V)$ est stable par φ et Γ_K, il suffit de prendre une base de $D^+(V)$ sur $\mathbf{B}_K^+$ pour conclure.

Lemme III.5. — *Si V est une représentation p-adique de $\mathscr{G}_K$ et si M est un sous-$\mathbf{A}_K^+$-module de type fini de $D(V)$ stable par φ, alors $M \subset D^+(V)$.*

Démonstration. — Soit T un $\mathbf{Z}_p$-réseau de V stable par $\mathscr{G}_K$. Quitte à multiplier M par une puissance de p, on peut supposer $M \subset D(T)$, ce que nous ferons. Si $x \in \widetilde{\mathbf{A}}$ et $n \in \mathbf{N}$, soit

$$w_n(x) = \inf\{v_{\mathbf{E}}(\alpha) \mid \alpha \in \widetilde{\mathbf{E}}^+ \text{ et } [\alpha]x \in \widetilde{\mathbf{A}}^+ + p^{n+1}\widetilde{\mathbf{A}}\}.$$

Soit $v_1, \ldots, v_d$ une base de T sur $\mathbf{Z}_p$. Si $x = x_1v_1 + \cdots + x_dv_d \in \widetilde{\mathbf{A}} \otimes T$ et $n \in \mathbf{N}$, posons $w_n(x) = \sup_{1 \leqslant i \leqslant d} w_n(x_i)$. Les propriétés suivantes sont immédiates.

i) Si $x \in \widetilde{\mathbf{A}} \otimes T$ et $n \in \mathbf{N}$, alors $w_n(x) \geqslant 0$ et $w_n(x) \leqslant w_{n+1}(x)$.

ii) Un élément x de $D(T)$ appartient à $D^+(T)$ si et seulement si $w_n(x) = 0$ quel que soit $n \in \mathbf{N}$.

iii) Si $x, y \in \widetilde{\mathbf{A}} \otimes T$ et $n \in \mathbf{N}$, alors $w_n(x+y) \leqslant \sup(w_n(x), w_n(y))$.

iv) Si $x \in \widetilde{\mathbf{A}} \otimes T$, $n \in \mathbf{N}$ et $a \in \mathbf{A}_K^+$, alors $w_n(ax) \leqslant w_n(x)$.

v) Si $x \in \widetilde{\mathbf{A}} \otimes T$ et $n \in \mathbf{N}$, alors $w_n(\varphi(x)) = pw_n(x)$.

Soient alors $e_1, \ldots, e_r$ des éléments engendrant M sur $\mathbf{A}_K^+$. En utilisant le fait que M est stable par φ et les propriétés ii) iii) et v), on obtient la majoration

$$w_n(e_i) = \frac{1}{p} w_n(\varphi(e_i)) \leqslant \frac{1}{p} \sup_{1 \leqslant j \leqslant r} w_n(e_j),$$

valable quels que soient $n \in \mathbf{N}$ et $1 \leqslant i \leqslant r$. On en déduit alors, utilisant la propriété i) pour la minoration, l'encadrement

$$0 \leqslant \sup_{1 \leqslant j \leqslant r} w_n(e_j) \leqslant \frac{1}{p} \sup_{1 \leqslant j \leqslant r} w_n(e_j),$$

ce qui, utilisant la propriété ii) permet de prouver que les e_i appartiennent à $D^+(T)$ et permet de conclure.

Corollaire III.6. — *Si $D(V)$ est de hauteur finie, alors V est de hauteur finie.*

Démonstration. — Soit $e_1, \ldots, e_d$ une base de $D(V)$ sur $\mathbf{B}_K$ telle que le sous-$\mathbf{B}_K^+$-module M de $D(V)$ engendré par $e_1, \ldots, e_d$ soit stable par φ. Comme on a supposé que $e_1, \ldots, e_d$ forment une base de $D(V)$ sur $\mathbf{B}_K$, il existe $N \in \mathbf{N}$ tel que $D(T) \subset p^{-N}(\mathbf{A}_K e_1 + \cdots + \mathbf{A}_K e_d)$ et donc, comme $B_K^+ \cap p^{-N}\mathbf{A}_K = p^{-N}\mathbf{A}_K^+$, le $\mathbf{A}_K^+$-module $M_0 = M \cap D(T)$ est inclus dans $p^{-N}(\mathbf{A}_K^+ e_1 + \cdots + \mathbf{A}_K^+ e_d)$ et donc de type fini puisque $\mathbf{A}_K^+$ est noethérien. D'autre part, comme il est stable par φ, il est inclus dans $D^+(V)$ d'après le ii) du lemme précédent. De plus, il existe $c \in \mathbf{N}$ tel que M_0 contienne $p^c e_1, \ldots, p^c e_d$, ce qui prouve que $D^+(V)$ contient une base de $D(V)$ sur $\mathbf{B}_K$ et permet de conclure.

Remarque III.7. — Dans [**4**, Chap. I, §6] une variante de w_n est introduite pour laquelle il est affirmé que l'on a $w_n(\varphi(x)) \leqslant p w_n(x)$, ce qui est faux mais cette propriété n'est pas utilisée dans le reste de [**4**]

L'équivalence des propriétés i) et ii) de la proposition III.2 résulte des corollaires III.4 et III.6.

3. (φ, Γ_K)**-modules essentiellement de hauteur finie.**— Ce paragraphe est consacré à la démonstration de l'équivalence des ii) et iii) de la proposition III.2. L'implication ii)⇒iii) résulte des corollaires III.4 et III.6. On peut reformuler la propriété iii) sous la forme

iii') Il existe un sous-groupe ouvert Γ de Γ_K et une base $f_1, \ldots, f_d$ de $D(V)$ sur $\mathbf{B}_K$ et $\lambda \in \mathbf{B}_K^+ - \{0\}$ tels que le sous-$\mathbf{B}_K^+$-module D^+ de $D(V)$ engendré par $f_1, \ldots, f_d$ soit stable par Γ et vérifie $\varphi(D^+) \subset \lambda^{-1} D^+$.

Pour prouver iii')→ii), il suffit de trouver $\alpha \in \mathbf{B}_K^+ - \{0\}$ tel que $\varphi(\alpha D^+) \subset \alpha D^+$ car alors la base $\alpha f_1, \ldots, \alpha f_d$ de $D(V)$ sur $\mathbf{B}_K$ vérifie les conditions voulues pour un (φ, Γ_K)-module de hauteur finie.

L'ensemble des $\lambda \in \mathbf{B}_K^+$ tels que $\lambda \varphi(D^+) \subset D^+$ est un idéal de $\mathbf{B}_K^+$ qui est stable par Γ puisque D^+ l'est par hypothèse et que φ commute à l'action de Γ. Nous aurons besoin du lemme suivant.

Lemme III.8. — *Les seuls idéaux de $\mathbf{B}_K^+$ stables par Γ sont engendrés par un élément de la forme $\pi^a \prod_n (\varphi^n(q))^{b_n}$, où a et les b_n sont des entiers presque tous nuls et $q = \frac{\varphi(\pi)}{\pi}$.*

Démonstration. — Pour la commodité du lecteur, nous reproduisons la démonstration de ce lemme que l'on peut trouver par exemple dans [**15**]. L'application qui à F associe $F(\pi)$ induit un isomorphisme de $\mathscr{B}_K^{[0,1)}$ sur $\mathbf{B}_K^+$. D'après le lemme II.3, les idéaux de $\mathscr{B}_K^{[0,1)}$ sont en bijection avec les polynômes unitaires à coefficients dans K dont toutes les racines α vérifient $0 \leqslant |\alpha| < 1$. Soit P un tel polynôme et soient $\beta_1, \ldots, \beta_m$ ses racines. Si l'idéal engendré par P est stable par Γ, alors $P(X)$ divise $P((1+X)^{\chi(\gamma)}-1)$ dans $\mathscr{B}_K^{[0,1)}$. Comme les racines de l'équation $P((1+X)^{\chi(\gamma)}-1) = 0$

vérifiant $0 \leqslant |\alpha| < 1$ sont les $(1+\beta_i)^{\chi(\gamma)^{-1}} - 1$, on en déduit le fait que l'application $\beta \rightarrow (1+\beta)^{\chi(\gamma)^{-1}} - 1$ est une bijection de l'ensemble des racines de P et donc que l'application $\beta \rightarrow (1+\beta)^{\chi(\gamma)^{-m!}} - 1$ est l'identité sur l'ensemble des racines de P et donc que les racines de P sont de la forme $\eta - 1$ ou η est une racine de l'unité d'ordre une puissance de p car $|\eta - 1| < 1$. Ceci implique que P peut se factoriser sous la forme $\prod P_n^{a_n}$, où $P_n(X-1)$ est le polynôme cyclotomique d'ordre p^n, c'est-à-dire, $P_0(X) = X$ et $P_n(X) = 1 + (1+X)^{p^{n-1}} + \cdots + (1+X)^{(p-1)p^{n-1}}$.

Réciproquement, P_n vérifie la condition "$P(X)$ divise $P((X+1)^{\chi(\gamma)} - 1)$", ce qui prouve que tout polynôme P de la forme $\prod P_n^{a_n}$ engendre un idéal de $\mathscr{B}_K^{[0,1)}$ stable par Γ. Pour terminer la démonstration du lemme, il suffit de constater l'on a $P_0(\pi) = \pi$ et $P_n(\pi) = \varphi^{n-1}(q)$ si $n \geqslant 1$.

Revenons à la démonstration de l'implication iii')$\rightarrow$ii). D'après le lemme précédent, on peut supposer que λ est de la forme $\pi^a \prod_{i=0}^n (\varphi^i(q))^{b_n}$. Comme on a $\varphi(\pi) = \pi q$, on voit que si l'on pose $\alpha = \pi^{b_0 + \cdots + b_n} q^{b_1 + \cdots b_n} \ldots \varphi^{n-1}(q)^{b_n}$, alors on a $\varphi(\alpha D^+) \subset \pi^{-a} \alpha D^+$. Pour conclure, il suffit d'appliquer le lemme suivant à $M = \alpha D^+$.

Lemme III.9. — *Soit M un $\mathbf{B}_K^+$-module libre de rang fini muni d'une action de Γ tel que le $\mathbf{B}_K^+[\frac{1}{\pi}]$-module $M[\frac{1}{\pi}]$ soit muni d'une action de φ commutant à celle de Γ et telle qu'il existe $a \in \mathbf{N}$ tel que l'on ait $\varphi(M) \subset \pi^{-a} M$. Alors $\varphi(M) \subset M$.*

Démonstration. — Soit $a \in \mathbf{N}$ l'entier minimal tel que $\varphi(M) \subset \pi^{-a} M$. Comme $\mathbf{B}_K^+ / \pi \mathbf{B}_K^+ = K$, on peut voir $M/\pi M$ comme un K-espace vectoriel de dimension $d = \dim_{\mathbf{B}_K^+} M$. Comme on a

$$\gamma(\pi) = \chi(\gamma)\pi \bmod \pi^2 \quad \text{et} \quad \varphi(\pi) = \pi q,$$

les applications γ et $\pi^a \varphi$ passent au quotient. Notons u l'application linéaire (car γ fixe K) induite par γ sur $M/\pi M$ et v l'application semi-linéaire induite par $\pi^a \varphi$. L'action de γ étant bijective, u est inversible et a ayant été choisi minimal, v est non nulle. Le fait que γ et φ commutent et la relation $\frac{\gamma(\pi)}{\pi} \cong \chi(\gamma) \bmod \pi$ se traduisent par la relation $u \circ v = \chi(\gamma)^{-a} v \circ u$. On peut aussi considérer $M/\pi M$ comme un $\mathbf{Q}_p$-espace vectoriel de dimension finie $d[K : \mathbf{Q}_p]$ et u et v comme des endomorphisme $\mathbf{Q}_p$-linéaires de $D^+/\pi D^+$ auquel cas, $u \circ v$ et $v \circ u$ ont même polynôme minimal et l'identité $u \circ v = \chi(\gamma)^{-a} v \circ u$ implique que $u \circ v = v \circ u = 0$, ce qui est impossible car u est inversible et v non-nulle grâce au choix de a, ou que $\chi(\gamma)^{-a}$ est une racine de l'unité et donc $a = 0$, ce qui permet de conclure.

4. (φ, Γ_K)-modules presque de hauteur finie.— Pour terminer la démonstration de la proposition III.2, il s'agit de démontrer l'équivalence des propriétés iii) et iv). Comme iii)$\Rightarrow$iv) de manière immédiate, il suffit de prouver iv)$\Rightarrow$iii). Soit $e_1, \ldots, e_d$ une base de $D(V)$ sur $\mathbf{B}_K$ telle que le $\mathrm{Fr}(\mathbf{B}_K^+)$-espace vectoriel W engendré par $e_1, \ldots, e_d$ soit stable par φ et Γ_K. Il s'agit de construire à l'intérieur de W un sous-$\mathbf{B}_K^+$-réseau stable par Γ_K. On peut aussi, utilisant le cocycle $\sigma \rightarrow U_\sigma$, où U_σ est la matrice de $\sigma \in \Gamma$ dans la base $e_1, \ldots, e_d$, reformuler le problème en termes de cohomologie des groupes et se ramener à démontrer la proposition suivante.

Proposition III.10. — *Si on munit $\mathbf{B}_K^+$ et $\mathrm{Fr}(\mathbf{B}_K^+)$ de la topologie induite par celle de $\mathbf{B}_K$, l'inclusion de $\mathbf{B}_K^+$ dans $\mathrm{Fr}(\mathbf{B}_K^+)$ induit une surjection d'ensembles de cohomologie continue de $H^1(\Gamma, \mathrm{GL}_d(\mathbf{B}_K^+))$ sur $H^1(\Gamma, \mathrm{GL}_d(\mathrm{Fr}(\mathbf{B}_K^+)))$.*

Démonstration. — La démonstration de cette proposition se fait en deux étapes : on utilise la continuité du cocycle et la compacité de Γ pour borner les dénominateurs des coordonnées de U_σ indépendamment de $\sigma \in \Gamma$, ce qui nous permet de nous ramener à une situation où la topologie est discrète (proposition III.13).

Le ii) de la proposition II.5 et le lemme II.4 montrent que si $b \in \mathbf{B}_K^+ - \{0\}$, alors $\mathbf{B}_K^+/b\mathbf{B}_K^+$ est un K-espace vectoriel de dimension finie. On notera $\|b\|$ cette dimension.

Lemme III.11. — *L'application qui à $x = \frac{a}{b} \in \mathrm{Fr}(\mathbf{B}_K^+)$, où a, b sont des éléments de $\mathbf{B}_K^+$ premiers entre eux, associe $\mathrm{ht}(x) = \|b\|$, est semi-continue inférieurement ($\mathrm{Fr}(\mathbf{B}_K^+)$ étant muni de la topologie induite par celle de $\mathbf{B}_K$).*

Démonstration. — Comme ht ne prend que des valeurs isolées (et même entières), il s'agit de prouver que si x_n est une suite d'éléments de $\mathrm{Fr}(\mathbf{B}_K^+)$ convergeant dans $\mathbf{B}_K$ vers $x = \frac{a}{b} \in \mathrm{Fr}(\mathbf{B}_K^+)$, alors $\mathrm{ht}(x_n) \geqslant \mathrm{ht}(x)$ si n est assez grand. D'après le lemme II.4 et le ii) de la proposition II.5, on peut écrire x_n sous la forme $\frac{a_n}{b_n}$, avec $a_n \in \mathbf{B}_K^+$ et $b_n = P_n(\pi)$ où P_n est un polynôme unitaire à coefficients dans l'anneau des entiers de K et de degré $\mathrm{ht}(x_n)$. Par hypothèse, la suite $x - x_n$ tend vers 0 dans $\mathbf{B}_K$ et comme on s'est débrouillé pour que $b_n \in \mathbf{A}_K^+$, la suite de terme général $bb_n(x-x_n) = ab_n - ba_n$ tend vers 0 dans $\mathbf{B}_K$. Comme de plus, cette suite est une suite d'éléments de $\mathbf{B}_K^+$ et que la topologie de $\mathbf{B}_K^+$ est la topologie induite par celle de $\mathbf{B}_K$, on en déduit le fait que la suite de terme général $ab_n - ba_n$ tend vers 0 dans $\mathbf{B}_K^+$ et donc aussi dans $\mathbf{B}_K^+/b\mathbf{B}_K^+$. Si on a supposé $(a, b) = 1$, on obtient finalement le fait que b_n tend vers 0 dans $\mathbf{B}_K^+/b\mathbf{B}_K^+$. L'idéal $b\mathbf{B}_K^+$ étant fermé dans $\mathbf{B}_K^+$, le K-espace vectoriel $\mathbf{B}_K^+/b\mathbf{B}_K^+$ qui est de de dimension finie $\|b\|$, est séparé et comme d'autre part, l'application qui à un polynôme $P \in F[X]$ de degré inférieur ou égal à $\|b\| - 1$ associe l'image de $P(\pi)$ dans $\mathbf{B}_K^+/b\mathbf{B}_K^+$ est bijective continue donc bicontinue et comme $b_n = P_n(\pi)$, où P_n est un polynôme unitaire, cela implique $\deg P_n = \mathrm{ht}(x_n) \geqslant \|b\| = \mathrm{ht}(x)$ si n est assez grand, ce qui permet de conclure.

Si $U = (a_{i,j})_{1\leqslant i,j\leqslant d} \in \mathrm{M}_d(\mathrm{Fr}(\mathbf{B}_K^+))$, posons $\mathrm{ht}(U) = \sum_{1\leqslant i,j\leqslant d} \mathrm{ht}(a_{i,j})$.

Corollaire III.12. — *Si $\sigma \to U_\sigma$ est un cocycle de Γ dans $\mathrm{GL}_d(\mathrm{Fr}(\mathbf{B}_K^+))$ continu pour la topologie de $\mathbf{B}_K$, alors il existe $m \in \mathbf{N}$ tel que $\mathrm{ht}(U_\sigma) \leqslant m$, quel que soit $\sigma \in \Gamma$.*

Démonstration. — D'après le lemme précédent, l'application qui à $\sigma \in \Gamma$ associe $\mathrm{ht}(U_\sigma)$ est semi-continue inférieurement et $X_n = \{\sigma \in \Gamma \mid \mathrm{ht}(U_\sigma) \leqslant n\}$ est donc fermé. Comme Γ est homéomorphe à un sous-groupe fermé de $\mathbf{Z}_p^*$, il est complet et comme $\bigcup_{n\in\mathbf{N}} X_n = \Gamma$, d'après le théorème de Baire, il existe $n \in \mathbf{N}$ tel que X_n soit d'intérieur non vide. Autrement dit, il existe $m_0 \in \mathbf{N}$ et O ouvert non vide de Γ tels que l'on ait $\mathrm{ht}(U_\sigma) \leqslant m_0$ si $\sigma \in O$. D'autre part, la relation de cocycle implique que $\mathrm{ht}(U_{\sigma\tau}) = \mathrm{ht}(U_\sigma \sigma(U_\tau)) \leqslant d^2(\mathrm{ht}(U_\sigma) + \mathrm{ht}(U_\tau))$ puisque tous les coefficients $a_{i,j}$ de $U_{\sigma\tau}$ vérifient l'inégalité $\mathrm{ht}(a_{i,j}) \leqslant \mathrm{ht}(U_\sigma) + \mathrm{ht}(U_\tau)$ comme on le constate en réduisant tout au même dénominateur (cette majoration est assez brutale, mais elle nous suffira). Pour conclure, il suffit alors de remarquer que Γ étant compact, il est réunion d'un nombre fini de translatés $\tau_1 O, \ldots, \tau_k O$ de O et que l'on a $\mathrm{ht}(U_\sigma) \leqslant d^2(\mathrm{ht}(U_{\tau_i}) + m_0)$ si $\sigma \in \tau_i O$ et donc que l'on peut prendre $m = d^2(\sup_i \mathrm{ht}(U_{\tau_i}) + m_0)$.

Proposition III.13. — *Soient A un anneau de Dedekind de corps des fractions L, I le groupe des idéaux fractionnaires de L, γ un automorphisme de A, G le sous-groupe de $\mathrm{Aut}(A)$ engendré* *par* γ *et* $\| \ \| : I \to \mathbf{Z}$ *un homomorphisme vérifiant* $\|\mathfrak{p}\| > 0$ *et* $\|\gamma(\mathfrak{p})\| = \|\mathfrak{p}\|$ *pour tout idéal maximal de* A*. Si* $U \in H^1(G, \mathrm{GL}_d(L))$*, les trois conditions suivantes sont équivalentes.*

i) U *est dans l'image de* $H^1(G, \mathrm{GL}_d(A))$*.*

ii) Quel que soit le cocycle $\sigma \to U_\sigma$ *de* G *dans* $\mathrm{GL}_d(L)$ *représentant* U*, il existe* $m \in \mathbf{N}$ *tel que, quel que soit* $\sigma \in G$*, il existe* $a_\sigma \in A - \{0\}$ *vérifiant* $\|(a_\sigma)\| \leqslant m$ *et* $a_\sigma U_\sigma \in \mathrm{M}_d(A)$*.*

iii) Il existe un cocycle $\sigma \to U_\sigma$ *de* G *dans* $\mathrm{GL}_d(L)$ *représentant* U *et* $m \in \mathbf{N}$ *tels que, quel que soit* $\sigma \in G$*, il existe* $a_\sigma \in A - \{0\}$ *vérifiant* $\|(a_\sigma)\| \leqslant m$ *et* $a_\sigma U_\sigma \in \mathrm{M}_d(A)$*.*

Avant de démontrer cette proposition, appliquons la à l'anneau principal $A = \mathbf{B}_K^+$ et à l'homomorphisme $\| \ \|$ défini par $\|(a)\| = \dim_K \mathbf{B}_K^+/(a)$ si $a \neq 0$ pour en déduire la proposition III.10. Soit γ un générateur topologique de Γ et G le sous-groupe discret de Γ engendré par γ. D'après le corollaire III.12, la restriction du cocycle $\sigma \to U_\sigma$ à G vérifie la propriété du iii) de la proposition III.13 ; il existe donc $M \in \mathrm{GL}_d(\mathrm{Fr}(\mathbf{B}_K^+))$ tel que $V_\sigma = M^{-1}U_\sigma\sigma(M) \in \mathrm{GL}_d(\mathbf{B}_K^+)$ quel que soit $\sigma \in G$. Le cocycle $\sigma \to V_\sigma$ étant continu sur Γ dans lequel G est dense et $\mathbf{B}_K^+$ étant fermé dans $\mathbf{B}_K$ et donc aussi dans $\mathrm{Fr}(\mathbf{B}_K^+)$, on a $V_\sigma \in \mathrm{GL}_d(\mathbf{B}_K^+)$ quel que soit $\sigma \in \Gamma$ et donc $\sigma \to U_\sigma$ est dans l'image de $H^1(\Gamma, \mathrm{GL}_d(\mathbf{B}_K^+))$, ce qu'il fallait démontrer.

Passons à la démonstration de la proposition III.13 et posons $\|a\| = \|(a)\|$ si $a \in A - \{0\}$. Par définition, si U est dans l'image de $H^1(G, \mathrm{GL}_d(L))$ et $\sigma \to U_\sigma$ est un cocycle représentant U, il existe $M \in \mathrm{GL}_d(A)$ et $\sigma \to V_\sigma$ un 1-cocycle à valeurs dans $\mathrm{GL}_d(A)$ tels que l'on ait $U_\sigma = M^{-1}V_\sigma\sigma(M)$ quel que soit $\sigma \in G$. Soient $a, a' \in A - \{0\}$ tels que aM^{-1} et $a'M$ appartiennent à $\mathrm{M}_d(A)$ et $m = \|a\| + \|a'\|$. Si $\sigma \in G$, soit $a_\sigma = a\sigma(a')$. Par construction, on a $a_\sigma U_\sigma = (aM^{-1})V_\sigma\sigma(a'M) \in \mathrm{M}_d(A)$ et comme $\|\sigma(x)\| = \|x\|$, cela implique que $\|a_\sigma\| \leqslant m$ quel que soit $\sigma \in G$, ce qui permet de démontrer l'implication i)$\Rightarrow$ii). Comme l'implication ii)$\Rightarrow$iii) est immédiate, il ne reste plus qu'à démontrer iii)$\Rightarrow$i).

Soit donc $\sigma \to U_\sigma$ un cocycle de G dans $\mathrm{GL}_d(L)$ représentant U et $m \in \mathbf{N}$ tels que, quel que soit $\sigma \in G$, il existe $a_\sigma \in A - \{0\}$ vérifiant $\|a_\sigma\| \leqslant m$ et $a_\sigma U_\sigma \in \mathrm{M}_d(A)$. On peut munir L^d d'une action semi-linéaire de G, la matrice U_σ représentant l'action de σ dans la base canonique de L^d. La condition $a_\sigma U_\sigma \in \mathrm{M}_d(A)$ se traduit par le fait que si T désigne le sous-réseau A^d de L^d, alors $\sigma(T) \subset a_\sigma^{-1}T$. Si σ, τ sont deux éléments de G, on a donc $\sigma\tau(T) = \sigma(\tau(T)) \subset \sigma(a_\tau^{-1}T) \subset a_\sigma^{-1}\sigma(a_\tau)^{-1}T$, ce qui implique que l'on peut supposer, quitte à remplacer a_σ par un diviseur, ce qui ne modifie pas la condition $\|a_\sigma\| \leqslant m$, que $a_{\sigma\tau}$ divise $a_\sigma\sigma(a_\tau)$ quels que soient $\sigma, \tau \in G$.

Soit Orb l'ensemble des orbites d'idéaux maximaux de A sous l'action de G. Si $X \in \mathrm{Orb}$ et $a \in A - \{0\}$, on pose $\pi_X(a) = \prod_{\mathfrak{p} \in X} \mathfrak{p}^{v_\mathfrak{p}(a)}$, ce qui fait que $\pi_X(a)$ est nul pour presque tout $X \in \mathrm{Orb}$ et $(a) = \prod_{X \in \mathrm{Orb}} \pi_X(a)$.

Comme G est engendré comme monoïde par γ et γ^{-1}, la condition "$a_{\sigma\tau}$ divise $a_\sigma\sigma(a_\tau)$" implique en particulier que si $X \in \mathrm{Orb}$ est telle que $\pi_X(a_\gamma) = \pi_X(a_{\gamma^{-1}}) = 0$, alors $\pi_X(a_\sigma) = 0$ quel que soit $\sigma \in G$. En particulier, l'ensemble Orb_U des éléments X de Orb tels qu'il existe $\sigma \in G$ tel que $\pi_X(a_\sigma) \neq 0$ est fini. Notons Orb_U^∞ (resp. Orb_U^f) l'ensemble des éléments de Orb_U de cardinal infini (resp. fini).

Soit maintenant $X \in \mathrm{Orb}_U^\infty$ et $\mathfrak{p}_0 \in X$. On définit une suite double $(\alpha_{n,i})_{n \geqslant 1, i \in \mathbf{Z}}$ d'éléments de $\mathbf{N}$ par la formule $\pi_X(a_{\gamma^n}) = \prod_{i \in \mathbf{Z}} \gamma^i(\mathfrak{p}_0)^{\alpha_{n,i}}$. La condition $\|a_{\gamma^n}\| \leqslant m$ implique que l'on a $\sum_{i \in \mathbf{Z}} \alpha_{n,i} \leqslant m$ quel que soit $n \geqslant 1$ et le fait que $a_{\gamma^{n_1+n_2}}$ divise $a_{\gamma^{n_1}}\gamma^{n_1}(a_{\gamma^{n_2}})$ se traduit par les inégalités $\alpha_{n_1+n_2,i} \leqslant \alpha_{n_1,i} + \alpha_{n_2,i-n_1}$ quels que soient $n_1, n_2 \geqslant 1$ et $i \in \mathbf{Z}$.

Lemme III.14. — *Soient $m \in \mathbf{N}$ et $(\alpha_{n,i})_{n\geqslant 1, i\in\mathbf{Z}}$ une suite double d'éléments de $\mathbf{N}$ vérifiant les conditions suivantes.*

i) $\sum_{i\in\mathbf{Z}} \alpha_{n,i} \leqslant m$ quel que soit $n \geqslant 1$.

ii) $\alpha_{n_1+n_2} \leqslant \alpha_{n_1,i} + \alpha_{n_2,i-n_1}$ quels que soient $n_1, n_2 \geqslant 1$ et $i \in \mathbf{Z}$.

Alors il existe $a, b, c \in \mathbf{N}$ tels que l'on ait $\alpha_{n,i} = 0$ si $i \notin [-c, a] \cup [n-b, n+c]$.

Démonstration. — Soit $c \in \mathbf{N}$ tel que l'on ait $\alpha_{1,i} = 0$ si $|i| > c$ (un tel c existe car la suite des $\alpha_{1,i}$ a au plus m termes non nuls). L'inégalité $\alpha_{n+1,i} \leqslant \alpha_{1,i} + \alpha_{n,i-1}$ permet de démontrer par récurrence sur n que $\alpha_{n,i} = 0$ si $i \notin [-c, n+c]$ (et même si $i \notin [-c, n+c-1]$).

Soit $n_0 \in \mathbf{N}$ tel qu'il existe $a \in [c, n_0 - c - 2]$ tel que $\alpha_{n_0,a} = \alpha_{n_0,a+1} = 0$ (comme $\alpha_{n,i}$ a au plus m termes non nuls, il suffit de prendre $n_0 \geqslant 2c + 3 + 2m$). Finalement, soit $b = n_0 - a - 2$, ce qui implique en particulier $b \geqslant c$. Montrons que l'on a $\alpha_{n,i} = 0$ si $a + 1 \leqslant i \leqslant n - b - 1$. La condition est vide si $n \leqslant n_0 - 1$. Si $n \geqslant n_0$, nous allons montrer par récurrence sur n que l'on a en fait $\alpha_{n,i} = 0$ si $i \in [a, n-b-1]$.

Si $n = n_0$, l'intervalle $[a, n-b-1]$ de $\mathbf{N}$ se réduit à $\{a, a+1\}$ et la propriété est vraie par construction de a. Si $n \in \mathbf{N}$, on déduit de la propriété iii) l'inégalité

$$\alpha_{n+1,i} \leqslant \inf(\alpha_{n,i} + \alpha_{1,n-i}, \alpha_{1,i} + \alpha_{n,i-1}).$$

Supposons donc que $n \geqslant n_0$ satisfait l'hypothèse de récurrence. Si $i \in [a, n-b-1]$, on a $\alpha_{n,i} = 0$ d'après l'hypothèse de récurrence et $\alpha_{1,i-n} = 0$ car $i - n \leqslant -b-1 \leqslant -c-1$, ce qui implique $\alpha_{n+1,i} = 0$. D'autre part, si $i = n - b$, on a $\alpha_{1,i} = 0$ car $n - b \geqslant a + 2 \geqslant c + 1$ et $\alpha_{n,i-1} = 0$ d'après l'hypothèse de récurrence. On a donc démontré que $n+1$ vérifie l'hypothèse de récurrence, ce qui permet de conclure.

Corollaire III.15. — *Si $\sigma \in G$, il existe $\alpha_\sigma, \beta_\sigma \in A - \{0\}$ tels $\sigma^n(\alpha_\sigma T) \subset \beta_\sigma^{-1} T$ quel que soit $n \in \mathbf{N}$.*

Démonstration. — D'après le lemme précédent, si $X \in \mathrm{Orb}_U^\infty$, il existe a_X, b_X, $c_X \in \mathbf{N}$ tels que si $\mathfrak{p}_X$ est un élément de X et $\pi_X(a_{\sigma^n}) = \prod_{k\in\mathbf{Z}} \gamma^k(\mathfrak{p}_X)^{\alpha_{X,n,k}}$, alors $\alpha_{X,n,k} = 0$ si $k \notin [-c_X, a_X] \cup [n - b_X, n + c_X]$. Comme d'autre part, $\alpha_{X,n,k} \leqslant m$ quels que soient X, n et k, si on pose

$$\mathfrak{a} = \prod_{X\in\mathrm{Orb}_U^\infty} \Big(\prod_{i=-b_X}^{c_X} \gamma^i(\mathfrak{p}_X) \Big) \quad \text{et} \quad \mathfrak{b} = \Big(\prod_{X\in\mathrm{Orb}_U^\infty} \Big(\prod_{i=-c_X}^{a_X} \gamma^i(\mathfrak{p}_X) \Big) \Big) \Big(\prod_{X\in\mathrm{Orb}_U^f} \prod_{\mathfrak{p}\in X} \mathfrak{p} \Big)$$

et si on choisit des éléments non nuls α et β de $\mathfrak{a}$ et $\mathfrak{b}$ respectivement, alors a_{σ^n} divise $\beta^m \sigma^n(\alpha^m)$ quel que soit $n \in \mathbf{N}$, ce qui fait que l'on peut prendre $\alpha_\sigma = \alpha^m$ et $\beta_\sigma = \beta^m$.

Revenons à la démonstration de la proposition III.13. Soient $e_1, \ldots, e_d$ la base canonique de L^d et T le sous-A-réseau de L^d engendré par $e_1, \ldots, e_d$. Soient $\alpha = \alpha_\gamma \alpha_{\gamma^{-1}}$ et $\beta = \beta_\gamma \beta_{\gamma^{-1}}$. Comme G est la réunion de $\gamma^{\mathbf{N}}$ et de $(\gamma^{-1})^{\mathbf{N}}$, il résulte du corollaire précédent que $\sigma(\alpha T) \subset \beta T$ quel que soit $\sigma \in G$ et donc que $\sum_{\sigma\in G} \sigma(\alpha T)$ est un sous-A-réseau de L^d stable par G. Ceci implique que la matrice de σ dans une base $f_1, \ldots, f_d$ de ce réseau appartient à $\mathrm{GL}_d(A)$ et que, si M est la matrice de passage de la base canonique de L^d à $(f_1, \ldots, f_d)$, alors le cocycle $\sigma \to M^{-1} U_\sigma \sigma(M)$ est à valeurs dans $\mathrm{GL}_d(A)$, ce qui permet de conclure.

Références

[1] D. Benois, On Iwasawa theory of cristalline representations, preprint 1998

[2] S. Bloch, K. Kato, L functions and Tamagawa numbers of motives. Dans "The Grothendieck Festchrift", vol. 1, 333-400, Prog. Math. **86**, Birkhaüser 1990

[3] F. Cherbonnier, P. Colmez, Représentations p-adiques surconvergentes, Inv. Math. **133**, 581-611, 1998

[4] F. Cherbonnier, P. Colmez, Théorie d'Iwasawa des représentations p-adiques d'un corps local, J. Amer. Math. Soc **12**, 241-268, 1999

[5] P. Colmez, Théorie d'Iwasawa des Représentations de de Rham d'un Corps Local, Ann. of Math. **148**, 485-571, 1998

[6] B. Dwork, G. Gerotto, F. Sullivan, An introduction to G-functions, Annals of Math. Studies 133, Princeton University Press, 1994

[7] J.-M. Fontaine, J.-P. Wintenberger, Le corps des normes de certaines extensions algébriques de corps locaux, C.R.A.S. **288**, 367-370, 1979

[8] J.-M. Fontaine, G. Laffaille, Construction de représentations p-adiques. Ann. Sci. E.N.S. 15, 547-608, 1982

[9] J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local ; construction d'un anneau de Barsotti-Tate. Ann. Math. **115**, 529-577, 1982

[10] J.-M. Fontaine, Représentations p-adiques des corps locaux, dans "The Grothendieck Festschrift", vol II, 249-309, Prog. Math. **87**, Birkhaüser 1991.

[11] J.-M. Fontaine, Le corps des périodes p-adiques. dans "Périodes p-adiques" exposé II, Astérisque **223**, 59-102, 1994

[12] J.-M. Fontaine, Représentations p-adiques semi-stables, dans "Périodes p-adiques" exposé III, Astérisque **223**, 113-184, 1994

[13] L. Herr, Cohomologie Galoisienne des corps p-adiques, thèse de l'université d'Orsay, 1995

[14] B. Perrin-Riou, Théorie d'Iwasawa des représentations p-adiques sur un corps local. Inv. Math. 115, 81-149, 1994

[15] N. Wach, Représentations p-adiques potentiellement cristallines, Bull. de la S.M.F. 124, 375-400, 1996

[16] N. Wach, Représentations cristallines de torsion, Comp. Math. 108, 185-240, 1997

[17] J.-P. Wintenberger, Le corps des normes de certaines extensions infinies des corps locaux ; applications, Ann. Sci. E.N.S. 16, 59-89, 1983

Pierre Colmez, Laboratoire de mathématiques, École normale supérieure, 45 rue d'Ulm, 75005 Paris, France
Institut de mathématiques de Jussieu, 4 place Jussieu, 75005 Paris, France • *E-mail :* `colmez@dmi.ens.fr`