

JEAN-PIERRE WINTENBERGER

Structure galoisienne de limites projectives d'unités locales

Séminaire de théorie des nombres de Grenoble, tome 7 (1978-1979), exp. n° 9, p. 1-19

http://www.numdam.org/item?id=STNG_1978-1979__7__A9_0

© Institut Fourier – Université de Grenoble, 1978-1979, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Grenoble

STRUCTURE GALOISIENNE DE LIMITES PROJECTIVES
D'UNITES LOCALES

par Jean-Pierre WINTENBERGER

1. - INTRODUCTION

Soit p un nombre premier et \mathbb{Q}_p le corps des nombres p -adiques. Soit K une extension finie de \mathbb{Q}_p . Soit K_∞ une extension abélienne de K . On note G le groupe de Galois de K_∞ sur K . On suppose que G est le produit direct d'un groupe Δ d'ordre premier à p et d'un groupe Γ isomorphe à \mathbb{Z}_p^r , pour r entier ≥ 1 . On note U_∞ (respectivement Z_∞) la limite projective des groupes des unités fondamentales (resp. des complétions p -adiques des groupes multiplicatifs : pour la définition voir 3) des extensions finies de K contenues dans K_∞ , les morphismes de transition étant induits par la norme. Les groupes U_∞ et Z_∞ sont de manière naturelle des modules sur l'algèbre Λ des mesures p -adiques sur G (l'algèbre Λ est aussi souvent appelée algèbre d'Iwasawa de G). Pour $r = 1$, la structure de ces modules a été étudiée par Iwasawa, cf. § 12 de [1]. Notre problème est d'étudier cette structure pour $r \geq 2$. Notre réponse est partielle, mais nous semble suffire pour les applications concernant les extensions abéliennes des corps quadratiques imaginaires (cf. un travail de Yager à paraître).

C'est avec plaisir que je remercie J.-M. Fontaine pour ses nombreux conseils. Mes plus vifs remerciements vont aussi à J. Coates pour l'intérêt qu'il a porté à ce travail et pour ses remarques lors de la rédaction. Je tiens à signaler que Coleman et Yager ont obtenu séparément des résultats (non publiés) sur le sujet.

2. - L'ALGÈBRE Λ DES MESURES p -ADIQUES SUR G .

Pour tout entier $n \geq 0$, on pose $G_n = G/p^n \Gamma$. On a :
 $\Lambda = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}_p[G_n]$, où $\mathbb{Z}_p[G_n]$ est l'algèbre sur \mathbb{Z}_p du groupe fini G_n . On identifie G à un sous-groupe du groupe des éléments inversibles de Λ .

On pose $A = \mathbb{Z}_p[\Delta]$. Comme Δ est d'ordre premier à p , les idempotents e_ϕ associés aux différents caractères irréductibles de Δ à valeur dans \mathbb{Q}_p , appartiennent à A . Si pour chaque ϕ , on pose $A_\phi = e_\phi A$ et $\Lambda_\phi = e_\phi \Lambda$, les algèbres A et Λ se décomposent respectivement en les produits $\prod_\phi A_\phi$ et $\prod_\phi \Lambda_\phi$. Pour chaque ϕ , $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A_\phi$ est l'extension non ramifiée de \mathbb{Q}_p de degré le degré ϕ et A_ϕ s'identifie à l'anneau de ses entiers. Soit $\sigma_1, \sigma_2, \dots, \sigma_r$ des générateurs de Γ (en tant que module sur \mathbb{Z}_p); on pose $T_i = \sigma_i - 1$ pour $1 \leq i \leq r$. L'algèbre Λ_ϕ s'identifie à l'algèbre des séries formelles $A_\phi[[T_1, T_2, \dots, T_r]]$.

Pour chaque ϕ , on munit Λ_ϕ de la topologie \mathfrak{m}_ϕ -adique, où \mathfrak{m}_ϕ est l'idéal maximal de Λ_ϕ . La topologie produit sur $\Lambda = \prod_\phi \Lambda_\phi$ coïncide avec la topologie limite projective $\Lambda = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}_p[G_n]$, les $\mathbb{Z}_p[G_n]$ étant munis de leur topologie p -adique.

Si M est un Λ -module, on pose $M_\phi = e_\phi M$. On a :
 $M = \prod_\phi M_\phi$, et pour $\phi \neq \phi'$ l'action de Λ_ϕ sur $M_{\phi'}$ est triviale.

3. - LES Λ -MODULES U_∞ et Z_∞ .

Si F est une extension finie de \mathbb{Q}_p , on appelle complétion p -adique du groupe multiplicatif de F et on note $\widehat{F^*}$ le groupe $\varprojlim_{t \in \mathbb{N}} F^*/F^{*p^t}$, la limite projective étant prise pour les applications évitentes. Le groupe $\widehat{F^*}$ est clairement un module sur \mathbb{Z}_p ; si π est une uniformisante de F , on a $\widehat{F^*} \simeq \pi \mathbb{Z}_p \times U_F^+$ où U_F^+ est le groupe des unités fondamentales de F .

Pour tout $n \in \mathbb{N}$, on désigne par K_n le corps des points fixes de K_∞ par $p^n \Gamma$. On a $Z_\infty = \varprojlim_{n \in \mathbb{N}} \widehat{K_n^*}$, les morphismes de transition étant induits par la norme. Pour chaque n , le groupe $\widehat{K_n^*}$ est de manière naturelle un module topologique compact sur $\mathbb{Z}_p[G_n]$. Par passage à la limite projective, on en déduit une structure de Λ -module topologique compact sur Z_∞ . Clairement, $U_\infty = \varprojlim_{n \in \mathbb{N}} U_{K_n}^+$ est un sous- Λ -module compact de Z_∞ .

4. - ENONCE DES RESULTATS.

On note $\bar{\chi}$ le caractère de Δ à valeurs dans les racines p -1-ième de l'unité de \mathbb{Q}_p , donnant l'action de Δ sur les racines p -ième de l'unité de K_∞ .

Si F est une extension de \mathbb{Q}_p , on note $\mu_{p^\infty}(F)$ le groupe des racines de l'unité de F d'ordre une puissance de p .

Si $\mu_{p^\infty}(K_\infty)$ est infini, pour tout $n \in \mathbb{N}$, on note μ_{p^n} le groupe des racines p^n -ième de l'unité de K_∞ . On note $T(\mu_{p^\infty})$ le module de Tate $\varprojlim_{n \in \mathbb{N}} \mu_{p^n}$. Pour chaque n , le groupe $\mu_{p^\infty}(K_n)$ est un module sur Λ par l'intermédiaire du quotient $\mathbb{Z}_p[G_n]$. Par passage à la limite projective, on en déduit une structure de Λ -module sur $T(\mu_{p^\infty})$.

Les homomorphismes d'augmentation : $\mathbb{Z}_p[G_n] \rightarrow \mathbb{Z}_p$, définissent un homomorphisme de Λ dans \mathbb{Z}_p . On note encore \mathbb{Z}_p le groupe \mathbb{Z}_p avec action de Λ à travers cet homomorphisme.

THEOREME. - On pose $d = [K:\mathbb{Q}_p]$. On note ϕ_0 le caractère trivial de Δ .

i) Supposons $r = 2$. Le Λ_{ϕ} -module $Z_{\infty, \phi}$ est libre de rang d , pour tout caractère irréductible ϕ de Δ si
 $\mu_{p^\infty}(K_\infty) = \{1\}$, et pour tout $\phi \neq \bar{\chi}$ si $\mu_{p^\infty}(K_\infty) \neq \{1\}$.
Si $\mu_{p^\infty}(K_\infty)$ est infini, et si $p \neq 2$ ou $\mu_4 \subset K$, on a une
suite exacte de $\Lambda_{\bar{\chi}}$ -modules :

$$(I) \quad 0 \rightarrow Z_{\infty, \bar{\chi}} \rightarrow L_{\bar{\chi}} \rightarrow T(\mu_{p^\infty}) \rightarrow 0,$$

où $L_{\bar{\chi}}$ est libre de rang d sur $\Lambda_{\bar{\chi}}$.

ii) Si $r \geq 3$, le Λ_{ϕ} -module $Z_{\infty, \phi}$ est libre de rang d pour
tout ϕ distinct de ϕ_0 et de $\bar{\chi}$.

iii) Pour r quelconque, on a $Z_{\infty, \phi} = U_{\infty, \phi}$, pour tout ϕ si
le corps résiduel de K_∞ est infini, et pour tout $\phi \neq \phi_0$
si le corps résiduel de K_∞ est fini. Dans le second cas,
et pour $\phi = \phi_0$, on a une suite exacte de Λ_{ϕ_0} -modules :

$$(II) \quad 0 \rightarrow U_{\infty, \phi_0} \rightarrow Z_{\infty, \phi_0} \rightarrow \mathbb{Z}_p \rightarrow 0.$$

Remarques.

1) Pour $r = 2$, $\mu_{p^\infty}(K_\infty)$ infini, et $p \neq 2$ ou $\mu_4 \subset K$, la suite exacte (I) décrit entièrement la structure de $\Lambda_{\bar{\chi}}$ -module de $Z_{\infty, \bar{\chi}}$. On voit facilement que l'on a $Z_{\infty, \bar{\chi}} \approx \mathcal{O} \oplus \Lambda_{\bar{\chi}}^{d-1}$, où \mathcal{O} est l'annulateur dans $\Lambda_{\bar{\chi}}$ de $T(\mu_{p^\infty})$.

2) De même, supposons $r = 2$ et le corps résiduel de K_∞ fini. Si $\mu_{p^\infty}(K_\infty) = \{1\}$ ou si $\mu_{p^\infty}(K_\infty) \neq \{1\}$ et $\bar{\chi} \neq \phi_0$ (c'est-à-dire si

$\mu_{p^\infty}(K) = \{1\}$), la suite exacte (II) décrit entièrement la structure de Λ_{Φ_0} -module de U_{∞, Φ_0} : on a $U_{\infty, \Phi_0} \approx \mathfrak{I}_{0, \Phi_0} \oplus \Lambda_{\Phi_0}^{d-1}$, où \mathfrak{I}_0 est l'idéal de Λ engendré par T_1 et T_2 .

3) Si $r \geq 3$, le Λ_{Φ_0} -module Z_{∞, Φ_0} n'est pas libre (voir la remarque du (5.5.1)).

PROPOSITION. - Notons \mathfrak{I}_0 l'idéal de Λ engendré par les T_i pour $1 \leq i \leq r$.

i) Pour r quelconque et $\Phi \neq \Phi_0$, le noyau de la projection de $Z_{\infty, \Phi}$ dans $\widehat{K}_{0, \Phi}^*$ est $\mathfrak{I}_0 Z_{\infty, \Phi}$.

ii) Pour $r = 2$, le noyau de l'homomorphisme de $Z_{\infty, \Phi_0} / \mathfrak{I}_0 Z_{\infty, \Phi_0}$ dans $\widehat{K}_{0, \Phi_0}^*$ induit par la projection est isomorphe à \mathbb{Z}_p .

5. - DEMONSTRATIONS.

(5.1) Interprétation par la théorie du corps de classe local. On se fixe une clôture algébrique de \mathbb{Q}_p et tous les corps considérés sont des sous-corps de cette clôture algébrique.

Si F est une extension finie de \mathbb{Q}_p , on pose $Z(F) = \widehat{F}^*$. Si F' est une extension finie de F , la norme induit un homomorphisme de $Z(F')$ dans $Z(F)$; on le désigne par $N_{F'/F}$. On note $M(F)$ la p -extension maximale abélienne de F . L'application d'Artin définit un isomorphisme :

$$(1) \quad \psi_F : Z(F) \xrightarrow{\sim} \text{Gal}(M(F)/F).$$

De plus, si F' est une extension finie de F , nous avons le diagramme commutatif classique :

$$(2) \quad \begin{array}{ccc} Z(F') & \xrightarrow{\psi_{F'}} & \text{Gal}(M(F')/F') \\ \downarrow N_{F'/F} & & \downarrow \\ Z(F) & \xrightarrow{\psi_F} & \text{Gal}(M(F)/F) \end{array}$$

où la flèche verticale de droite est l'homomorphisme naturel défini par l'inclusion $M(F) \subset M(F')$. Supposons de plus F'/F galoisienne. Comme $M(F')/F$ est alors galoisienne, $\text{Gal}(F'/F)$ opère sur $\text{Gal}(M(F')/F')$ par automorphismes intérieurs (si $\sigma \in \text{Gal}(F'/F)$ et $x \in \text{Gal}(M(F')/F')$, alors $\sigma \cdot x = \gamma x \gamma^{-1}$, où γ est un quelconque élément de $\text{Gal}(M(F')/F)$ dont l'image dans $\text{Gal}(F'/F)$ est σ). D'autre part, le groupe $\text{Gal}(F'/F)$ opère sur $Z(F')$ de manière naturelle. Il est bien connu que $\psi_{F'}$ est un $\text{Gal}(F'/F)$ -homomorphisme.

Si F est une extension algébrique quelconque de \mathbb{Q}_p , on note toujours $M(F)$ la p -extension maximale abélienne de F ; on pose $Z(F) = \varprojlim Z(E)$, où E décrit les extensions finies de \mathbb{Q}_p contenues dans F et où, pour $E \subset E'$, l'homomorphisme de transition est $N_{E'/E}$. Par passage à la limite, les faits rappelés ci-dessus concernant les extensions finies de \mathbb{Q}_p s'étendent aux extensions algébriques quelconques de \mathbb{Q}_p . En particulier, nous avons l'isomorphisme (1) et pour $F \subset F'$, le diagramme commutatif (2), où $N_{F'/F}$ est induit par les homomorphismes $N_{E/E \cap F}$, où E décrit les extensions finies de \mathbb{Q}_p contenues dans F' .

Revenons à notre extension K_∞ . Notons comme précédemment \mathfrak{A}_0 l'idéal de Λ engendré par T_1, T_2, \dots, T_r . Soit N le corps des points fixes de $M(K_\infty)$ par $\psi_{K_\infty}(\mathfrak{A}_0 Z_\infty)$. Comme $M(K_0)$ est une extension abélienne de K_0 , on a $(\sigma \cdot x)x^{-1} \in \text{Gal}(M(K_\infty)/M(K_0))$ pour tout $\sigma \in \Gamma$ et tout $x \in \text{Gal}(M(K_\infty)/K_\infty)$. Par suite $\psi_{K_\infty}(\mathfrak{A}_0 Z_\infty) \subset \text{Gal}(M(K_\infty)/M(K_0))$, et donc :

$$K_0 \subset K_\infty \subset M(K_0) \subset N \subset M(K_\infty).$$

Pour tout i avec $1 \leq i \leq r$, choisissons dans $\text{Gal}(N/K_0)$ un élément τ_i dont l'image dans $\Gamma = \text{Gal}(K_\infty/K_0)$ est σ_i . Comme $M(K_0)$ est l'extension maximale abélienne de K_0 contenue dans N , on voit facilement que $\text{Gal}(N/M(K_0))$ est engendré sur \mathbb{Z}_p par les $\theta_{i,i'}$ où, pour $1 \leq i < i' \leq r$: $\theta_{i,i'} = \tau_i \tau_{i'}^{-1} \tau_i^{-1} \tau_{i'}$.

Remarque. Il est vrai, mais plus délicat à prouver, que les $\theta_{i,i'}$ forment une base du \mathbb{Z}_p -module $\text{Gal}(N/M(K_0))$. Pour $r = 2$, cela résulte de la proposition du § 4.

(5.2) LEMME. - Soit F et F' deux extensions de K contenues dans K_∞ avec $F \subset F'$ et $\text{Gal}(F'/F) \approx \mathbb{Z}_p$. Soit σ un élément de G dont l'image dans $\text{Gal}(F'/K)$ est un générateur de $\text{Gal}(F'/F)$. Alors :

- i) le noyau de $N_{F'/F} : Z(F') \rightarrow Z(F)$ est $(\sigma-1)Z(F')$,
- ii) si Z' est l'image de $N_{F'/F}$, alors le quotient $Z(F)/Z'$ est isomorphe, en tant que Λ -module, à \mathbb{Z}_p (cf. 4),
- iii) la multiplication par $\sigma-1$ est injective dans $Z(F')$.

Démonstration du i). Soit P le corps des points fixes de $M(F')$ par $\psi_{F',((\sigma-1)Z(F'))}$. Il s'agit de montrer que $P = M(F)$. Clairement, $M(F) \subset P$. Tout revient donc à montrer que P/F est abélienne. Soit τ un élément de $\text{Gal}(P/F)$ dont l'image dans $\text{Gal}(F'/F)$ coïncide avec celle de σ . Pour tout $\gamma \in \text{Gal}(P/F')$ provenant via l'application d'Artin de $z \in Z(F')/(\sigma-1)Z(F')$, le commutateur $\tau\gamma\tau^{-1}\gamma^{-1}$ provient de $(\sigma-1)z$, qui clairement est nul. On voit donc que τ commute à tout élément de $\text{Gal}(P/F')$. Comme le groupe $\text{Gal}(P/F)$ est engendré par τ et les éléments de $\text{Gal}(P/F')$, il en résulte que $\text{Gal}(P/F)$ est commutatif. Cela prouve le i).

Démonstration du ii). On a la suite exacte :

$$1 \rightarrow \text{Gal}(M(F)/F') \rightarrow \text{Gal}(M(F)/F) \rightarrow \text{Gal}(F'/F) \rightarrow 1 .$$

Puisque F'/K est abélienne, G agit trivialement sur $\text{Gal}(F'/F)$ et la suite exacte ci-dessus donne la suite exacte de Λ -modules :

$$0 \rightarrow Z' \rightarrow Z(F) \rightarrow \mathbb{Z}_p \rightarrow 0 .$$

Cela prouve le ii).

Démonstration du iii). Supposons tout d'abord F/\mathbb{Q}_p finie. Dans ce cas, le résultat découle immédiatement du théorème d'Iwasawa, cf. th.25 de [1], donnant la structure de $Z(F')$ en tant que module sur l'algèbre des mesures sur $\text{Gal}(F'/F)$: si $\mu_{p^\infty}(F')$ est fini, le module $Z(F')$ se plonge dans un module libre (avec un quotient isomorphe à $\mu_{p^\infty}(F')$), si $\mu_{p^\infty}(F')$ est infini, le module $Z(F')$ est somme directe d'un module libre et du module de Tate $T(\mu_{p^\infty})$.

Passons au cas général. Choisissons E_0 et E'_0 extensions de K avec E_0/K finie, $E_0 \subset F$, $E_0 \subset E'_0 \subset F'$, $E'_0 \cap F = E_0$ et $E'_0 F = F'$. Pour chaque extension finie E de E_0 contenue dans F , il résulte du cas particulier précédemment traité que la multiplication par $\sigma - 1$ est injective dans $Z(E'_0 E)$. Comme $Z(F') = \varprojlim Z(E E'_0)$, il en résulte que la multiplication par $\sigma - 1$ est injective dans $Z(F')$. Cela achève la démonstration du lemme.

(5.3) Démonstration de la proposition.

Démonstration du i). Raisonnons par récurrence sur r . Pour $r = 1$, le noyau de $N_{K_\infty/K_0} : Z_\infty \rightarrow \widehat{K_{0, \Phi}^*}$ est $T_1 Z_\infty$, cf. i) du lemme précédent. Cela prouve le résultat dans ce cas.

Supposons $r \geq 2$. Notons F le corps des points fixes de K_∞ par σ_r et Z' l'image de Z_∞ dans $Z(F)$. Le noyau de $N_{K_\infty/F} : Z_\infty \rightarrow Z(F)$ est $T_r Z_\infty$, cf. i) du lemme précédent. On a donc $Z' \approx Z_\infty / T_r Z_\infty$. Comme, cf. ii) du lemme précédent, le quotient $Z(F)/Z'$ est isomorphe à \mathbb{Z}_p en tant que Λ -module, on a $Z(F)_{\Phi} = Z'_{\Phi}$, pour tout $\Phi \neq \Phi_0$. Alors, $Z(F)_{\Phi} \approx Z_{\infty, \Phi} / T_r Z_{\infty, \Phi}$ et :

$$Z_{\infty, \Phi} / \mathfrak{g}_0 Z_{\infty, \Phi} \approx Z(F)_{\Phi} / T_1 Z(F)_{\Phi} + \dots + T_{r-1} Z(F)_{\Phi}.$$

Comme, d'après l'hypothèse de récurrence, le noyau de la projection de $Z(F)_{\Phi}$ dans $\widehat{K_{0, \Phi}^*}$ est $T_1 Z(F)_{\Phi} + \dots + T_{r-1} Z(F)_{\Phi}$, on en

déduit que le noyau de la projection de $Z_{\infty, \Phi}$ dans $\widehat{K_{O, \Phi}^*}$ est $\mathcal{J}_O Z_{\infty, \Phi}$.
Cela prouve le i) .

Démonstration du ii). Soit F le corps des points fixes de K_{∞} par σ_2 . Notons Z' l'image de Z_{∞} dans $Z(F)$. On a, cf. ii) du lemme précédent, la suite exacte :

$$0 \rightarrow Z' \rightarrow Z(F) \rightarrow \mathbb{Z}_p \rightarrow 0 .$$

La multiplication par T_1 est injective dans $Z(F)$, cf. iii) du lemme précédent. On déduit alors de la suite exacte ci-dessus, la suite exacte :

$$0 \rightarrow \mathbb{Z}_p \rightarrow Z'/T_1 Z' \rightarrow Z(F)/T_1 Z(F) \rightarrow \mathbb{Z}_p \rightarrow 0 .$$

D'après le i) du lemme précédent, l'homomorphisme $N_{K_{\infty}/F}$ induit un isomorphisme de $Z_{\infty}/T_2 Z_{\infty}$ sur Z' ; de même, N_{F/K_O} induit une injection de $Z(F)/T_1 Z(F)$ dans $\widehat{K_{O, \Phi}^*}$. Par suite, la suite exacte ci-dessus donne :

$$0 \rightarrow \mathbb{Z}_p \rightarrow Z_{\infty}/T_1 Z_{\infty} + T_2 Z_{\infty} \rightarrow \widehat{K_{O, \Phi}^*} .$$

On en déduit que le noyau de l'homomorphisme de $Z_{\infty, \Phi}/\mathcal{J}_O Z_{\infty, \Phi}$ dans $\widehat{K_{O, \Phi}^*}$ est isomorphe à \mathbb{Z}_p . Cela achève la démonstration de la proposition.

(5.4) Un lemme concernant les modules sur les anneaux de séries formelles.

LEMME. Soit p un nombre premier. Soit B un anneau de valuation discrète d'idéal maximal \mathfrak{m} . On suppose que $p \in \mathfrak{m}$.

Soit $S = B[[X_1, X_2, \dots, X_k]]$ l'algèbre des séries formelles à coefficients dans B et en les k indéterminées X_1, X_2, \dots, X_k .

Pour tout entier j avec $1 \leq j \leq k$ et tout $n \in \mathbb{N}$, posons :

$s_{n,j} = (1+X_j)^{p^n} - 1$. Soit \mathfrak{M} l'idéal maximal de S . Soit M

un module sur S , séparé et complet pour sa topologie \mathfrak{M} -

adique. On suppose qu'il existe un entier h tel que, pour tout

$n \in \mathbb{N}$, le B-module $M/s_{n,1}M + s_{n,2}M + \dots + s_{n,k}M$ est libre de

rang hp^{kn} . Alors M est libre de rang h sur S .

Démonstration. Soit x_1, x_2, \dots, x_h des éléments de M relevant une base de $M/X_1M + X_2M + \dots + X_kM$ en tant que module sur B . Un raisonnement par approximations successives facile montre que les x_i engendrent M , en tant que module sur S . Considérons alors l'homomorphisme surjectif i de S -module de S^h dans M , qui à $(\alpha_1, \alpha_2, \dots, \alpha_h)$ associe $\sum_{i=1}^h \alpha_i x_i$. Pour tout $n \in \mathbb{N}$, il induit un homomorphisme surjectif i_n de $(S/s_{n,1}S + s_{n,2}S + \dots + s_{n,k}S)^h$ dans $M/s_{n,1}M + s_{n,2}M + \dots + s_{n,k}M$. Pour $1 \leq j \leq k$, le polynôme $s_{n,j}$ est un polynôme distingué de $B[[X_j]]$, le théorème de préparation de Weierstrass montre alors que $S/s_{n,1}S + s_{n,2}S + \dots + s_{n,k}S$ est libre de rang p^{nk} sur B . Par suite $(S/s_{n,1}S + s_{n,2}S + \dots + s_{n,k}S)^h$ est libre de rang hp^{nk} . Il en est de même de $M/s_{n,1}M + s_{n,2}M + \dots + s_{n,k}M$ par hypothèse. On voit donc que les i_n , dont on sait déjà qu'ils sont surjectifs, sont des isomorphismes.

Une récurrence facile montre que, puisque $p \in \mathfrak{m}$, on a $s_{n,j} \in \mathfrak{m}^{n+1}$. Comme S et M sont séparés et complets pour leur topologie \mathfrak{m} -adique, on en déduit que $S = \varprojlim_{n \in \mathbb{N}} S/s_{n,1}S + s_{n,2}S + \dots + s_{n,k}S$ et $M = \varprojlim_{n \in \mathbb{N}} M/s_{n,1}M + s_{n,2}M + \dots + s_{n,k}M$. Comme les i_n sont des isomorphismes, il en résulte que i est aussi un isomorphisme, et $M \cong S^h$. Cela prouve le lemme.

(5.5) Démonstration des i) et ii) du théorème.

Pour tout $n \in \mathbb{N}$ et tout i avec $1 \leq i \leq r$, on pose $\omega_{n,i} = (1+T_i)^{p^n} - 1$. Pour tout $n \in \mathbb{N}$, on note \mathfrak{J}_n l'idéal de A engendré par les $\omega_{n,i}$ pour $1 \leq i \leq r$.

(5.5.1) LEMME. - Soit $n \in \mathbb{N}$. Le $A_{\bar{\phi}}$ -module $Z_{\infty, \bar{\phi}} / \mathfrak{J}_n Z_{\infty, \bar{\phi}}$ est libre de rang dp^{nr} dans les cas suivants : si $r = 2$ et $\mu_{p^\infty}(K_\infty) = \{1\}$ pour tout $\bar{\phi}$, si $r = 2$ et $\mu_{p^\infty}(K_\infty) \neq \{1\}$ pour tout $\bar{\phi} \neq \bar{\chi}$, si $r \geq 3$ pour tout $\bar{\phi}$ distinct de $\bar{\chi}$ et de $\bar{\phi}_0$.

Si $r = 2$, le rang sur $A_{\bar{\chi}}$ de $Z_{\infty, \bar{\chi}} / \mathcal{J}_n Z_{\infty, \bar{\chi}}$ modulo torsion est dp^{2n} .

Démonstration. Pour tout $n \in \mathbb{N}$, notons Z_n l'image de Z_{∞} dans \widehat{K}_n^* . Si M est un module de type fini sur un anneau principal B , désignons par $\text{rg}_B(M)$ le rang de M modulo torsion.

Appliquons la proposition à l'extension de groupe de Galois $p^n \Gamma \times \Delta$: pour $r \geq 2$ et $\phi \neq \phi_0$, on a $Z_{n, \phi} \simeq Z_{\infty, \phi} / \mathcal{J}_n Z_{\infty, \phi}$; pour $r = 2$, le noyau de l'homomorphisme de $Z_{\infty, \phi_0} / \mathcal{J}_n Z_{\infty, \phi_0}$ dans \widehat{K}_n^* est isomorphe à \mathbb{Z}_p . On a donc :

$$(I) : \begin{cases} \text{rg}_{A_{\phi}}(Z_{\infty, \phi} / \mathcal{J}_n Z_{\infty, \phi}) = \text{rg}_{A_{\phi}}(Z_{n, \phi}) , & \text{pour } \phi \neq \phi_0 , \\ \text{rg}_{A_{\phi_0}}(Z_{\infty, \phi_0} / \mathcal{J}_n Z_{\infty, \phi_0}) = \text{rg}_{A_{\phi_0}}(Z_{n, \phi_0}) + 1 , & \text{pour } r = 2 . \end{cases}$$

Le groupe Z_n est isomorphe, par la théorie du corps de classe, à $\text{Gal}(M(K_n)/K_{\infty})$ et donc le quotient \widehat{K}_n^*/Z_n à $\text{Gal}(K_{\infty}/K_n)$. Par suite :

$$(II) : \begin{cases} \text{rg}_{A_{\phi}}(Z_{n, \phi}) = \text{rg}_{A_{\phi}}(\widehat{K}_{n, \phi}^*) , & \text{si } \phi \neq \phi_0 , \\ \text{rg}_{A_{\phi_0}}(Z_{n, \phi_0}) = \text{rg}_{A_{\phi_0}}(\widehat{K}_{n, \phi_0}^*) - r . \end{cases}$$

Soit \mathcal{O}_n l'anneau des entiers de K_n et U_n le groupe des unités fondamentales de K_n . On sait qu'il existe un sous $\mathbb{Z}_p[G_n]$ -module V_n de U_n d'indice fini tel que le logarithme p -adique induise un isomorphisme de V_n sur un sous- $\mathbb{Z}_p[G_n]$ -module d'indice fini de \mathcal{O}_n .

On a alors : $\text{rg}_{\mathbb{Z}_p}(U_{n, \phi}) = \text{rg}_{\mathbb{Z}_p}(V_{n, \phi}) = \text{rg}_{\mathbb{Z}_p}(\mathcal{O}_{n, \phi}) = \dim_{\mathbb{Q}_p}(K_{n, \phi})$.

Comme K_n est libre de rang d sur $\mathbb{Q}_p[G_n]$, on en déduit que $\text{rg}_{\mathbb{Z}_p}(U_{n, \phi}) = d[\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A_{\phi} : \mathbb{Q}_p] p^{rn}$, d'où : $\text{rg}_{A_{\phi}}(U_{n, \phi}) = dp^{rn}$ et :

$$(III) : \begin{cases} \text{rg}_{A_{\phi}}(\widehat{K}_{n, \phi}^*) = dp^{rn} , & \text{si } \phi \neq \phi_0 , \\ \text{rg}_{A_{\phi_0}}(\widehat{K}_{n, \phi_0}^*) = dp^{rn} + 1 . \end{cases}$$

De (I) , (II) et (III) résulte immédiatement que $\text{rg}_{A_{\bar{\phi}}} (Z_{\infty, \bar{\phi}} / \mathcal{J}_n Z_{\infty, \bar{\phi}}) = dp^{rn}$, pour tout $\bar{\phi}$ si $r = 2$, et pour tout $\bar{\phi} \neq \bar{\phi}_0$ si $r \geq 3$.

Pour $\mu_{p^\infty}(K_\infty) = \{1\}$ ou pour $\mu_{p^\infty}(K_\infty) \neq \{1\}$ et $\bar{\phi} \neq \bar{\chi}$, le $A_{\bar{\phi}}$ -module $Z_{n, \bar{\phi}}$ est sans torsion. Il en est de même de $Z_{\infty, \bar{\phi}} / \mathcal{J}_n Z_{\infty, \bar{\phi}}$ si $\bar{\phi} \neq \bar{\phi}_0$ ou $r = 2$, puisque $Z_{\infty, \bar{\phi}} / \mathcal{J}_n Z_{\infty, \bar{\phi}} \simeq Z_{n, \bar{\phi}}$ si $\bar{\phi} \neq \bar{\phi}_0$ et que pour $r = 2$, on a la suite exacte

$$0 \rightarrow \mathbb{Z}_p \rightarrow Z_{\infty, \bar{\phi}_0} / \mathcal{J}_n Z_{\infty, \bar{\phi}_0} \rightarrow Z_{n, \bar{\phi}_0} \rightarrow 0 .$$

Cela achève de prouver le lemme.

Remarque. On voit facilement que, comme le rang sur \mathbb{Z}_p du noyau de l'homomorphisme de $Z_\infty / \mathcal{J}_n Z_\infty$ dans \widehat{K}_n^* est $r(r-1)/2$, cf. remarque du (5.1), on a $\text{rg}_{\mathbb{Z}_p} (Z_{\infty, \bar{\phi}_0} / \mathcal{J}_n Z_{\infty, \bar{\phi}_0}) = dp^{rn} + \frac{(r-1)(r-2)}{2}$. Il en résulte que, pour $r > 2$, $Z_{\infty, \bar{\phi}_0}$ n'est pas libre sur $\Lambda_{\bar{\phi}_0}$.

(5.5.2) LEMME. - Pour $r = 2$ ou $r \geq 3$ et $\bar{\phi} \neq \bar{\phi}_0$, le $\Lambda_{\bar{\phi}}$ -module $Z_{\infty, \bar{\phi}}$ est de type fini.

Démonstration. Comme $Z_{\infty, \bar{\phi}}$ est compact et que, d'après le lemme précédent, $Z_{\infty, \bar{\phi}} / \mathcal{M}_{\bar{\phi}} Z_{\infty, \bar{\phi}}$ est de type fini sur $\Lambda_{\bar{\phi}} / \mathcal{M}_{\bar{\phi}}$, le lemme résulte d'une version topologique du lemme de Nakayama (voir par exemple p.126 de [2]).

(5.5.3) Examen des cas $r = 2$ et $\mu_{p^\infty}(K_\infty) = \{1\}$, $r = 2$ et $\bar{\phi} \neq \bar{\chi}$, $r \geq 3$ et $\bar{\phi}$ distinct de $\bar{\phi}_0$ et de $\bar{\chi}$.

Comme $Z_{\infty, \bar{\phi}}$ est de type fini, il est séparé et complet pour sa topologie $\mathcal{M}_{\bar{\phi}}$ -adique. Dans chacun des cas considérés, $Z_{\infty, \bar{\phi}} / \mathcal{J}_n Z_{\infty, \bar{\phi}}$ est libre sur $A_{\bar{\phi}}$ de rang dp^{rn} , cf. lemme (5.5.1) ; le lemme (5.4) montre alors que $Z_{\infty, \bar{\phi}}$ est libre de rang d sur $\Lambda_{\bar{\phi}}$.

(5.5.4) Examen du cas $r = 2$, $\mu_{p^\infty}(K_\infty)$ infini, $p \neq 2$ ou $\mu_4 \subset K$ et
 $\bar{\phi} = \bar{\chi}$.

On note χ le caractère de G à valeurs dans les unités de \mathbb{Z}_p donnant l'action de G sur μ_{p^∞} (on voit facilement que $\bar{\chi}$ est la restriction de χ à Δ). On choisit les générateurs σ_1 et σ_2 de Γ de telle sorte que σ_1 engendre le noyau de la restriction de χ à Γ . On note p^{m_0} le cardinal de $\mu_{p^\infty}(K_0)$.

Pour $n \in \mathbb{N}$, on note F_n le corps des points fixes de K_∞ par le groupe engendré par σ_2 et $\sigma_1^{p^n}$. (Donc $F_0 = K_0$; on voit facilement que $\mu_{p^\infty}(F_n) = \mu_{p^{m_0}}$ et que $F_n(\mu_{p^\infty})$ est le corps des points fixes de K_∞ par $\sigma_1^{p^n}$). Pour $m \geq m_0$, la restriction à $\mu_{p^{m+1}}$ de la norme de $F_n(\mu_{p^{m+1}})$ à $F_n(\mu_{p^m})$ est : $\xi \mapsto \xi^p$, si $p \neq 2$, et : $\xi \mapsto -\xi^2$, si $p = 2$. Dans tous les cas, on en déduit un homomorphisme injectif i_n de $T(\mu_{p^\infty})$ dans $Z(F_n(\mu_{p^\infty}))$.

LEMME. - Pour tout $n \in \mathbb{N}$, désignons par Z'_n l'image par
 $N_{K_\infty/F_n(\mu_{p^\infty})}$ de Z_∞ dans $Z(F_n(\mu_{p^\infty}))$ et par f_n l'homomorphisme
de $\text{Hom}_\Lambda(T(\mu_{p^\infty}), Z'_n)$ dans $\text{Ext}_\Lambda^1(T(\mu_{p^\infty}), Z_\infty)$ correspondant à la
suite exacte :

$$0 \rightarrow Z_\infty \xrightarrow{x_{n,1}} Z_\infty \rightarrow Z'_n \rightarrow 0.$$

i) On a $i_n(T(\mu_{p^\infty})) \subset Z'_n$.

ii) D'après le i), on a $i_n \in \text{Hom}_\Lambda(T(\mu_{p^\infty}), Z'_n)$; l'image de i_n par f_n ne dépend pas de n .

Démonstration. Montrons le i). Pour $m \geq m_0$, désignons par $Z'_{n,m}$ l'image de Z_∞ dans $\widehat{F_n(\mu_{p^m})}^*$. Le quotient $\widehat{F_n(\mu_{p^m})}^*/Z'_{n,m}$ est isomorphe, via l'application d'Artin, à $\text{Gal}(K_\infty/F_n(\mu_{p^m}))$. Il est donc sans torsion en tant que module sur \mathbb{Z}_p . Par suite μ_{p^m} est inclus dans $Z'_{n,m}$. Un argument de compacité facile prouve que $Z'_n = \varprojlim_{m \geq m_0} Z'_{n,m}$.

Il en résulte que $i_n(T(\mu_{p^\infty})) \subset Z'_n$. Cela prouve le i).

Montrons le ii). Soit n' un entier $\geq n$. Comme, sur $\widehat{F_{n', (\mu_{p^m})}^*}$, la multiplication par $\omega_{n', 1}/\omega_{n, 1}$ coïncide avec $N_{F_{n', (\mu_{p^m})}/F_n(\mu_{p^m})}$,

le diagramme suivant est commutatif:

$$(I) : \begin{array}{ccc} T(\mu_{p^\infty}) & \xrightarrow{i_n} & Z_\infty/\omega_{n, 1}Z_\infty \\ & \searrow i_{n'} & \downarrow \times \omega_{n', 1}/\omega_{n, 1} \\ & & Z_\infty/\omega_{n', 1}Z_\infty \end{array}$$

Le diagramme suivant est commutatif et ses lignes sont exactes :

$$\begin{array}{ccccccc} 0 & \longrightarrow & Z_\infty & \xrightarrow{\times \omega_{n, 1}} & Z_\infty & \longrightarrow & Z_\infty/\omega_{n, 1}Z_\infty \longrightarrow 0 \\ & & \parallel \text{Id} & & \downarrow \times \omega_{n', 1}/\omega_{n, 1} & & \downarrow \times \omega_{n', 1}/\omega_{n, 1} \\ 0 & \longrightarrow & Z_\infty & \xrightarrow{\times \omega_{n', 1}} & Z_\infty & \longrightarrow & Z_\infty/\omega_{n', 1}Z_\infty \longrightarrow 0 \end{array} .$$

Par suite :

$$\begin{array}{ccc} \text{Hom}_\wedge(T(\mu_{p^\infty}), Z_\infty/\omega_{n, 1}Z_\infty) & \xrightarrow{f_n} & \text{Ext}_\wedge^1(T(\mu_{p^\infty}), Z_\infty) \\ \downarrow \times \omega_{n', 1}/\omega_{n, 1} & & \parallel \text{Id} \\ \text{Hom}_\wedge(T(\mu_{p^\infty}), Z_\infty/\omega_{n', 1}Z_\infty) & \xrightarrow{f_{n'}} & \text{Ext}_\wedge^1(T(\mu_{p^\infty}), Z_\infty) \end{array} .$$

De (I) on déduit alors que $f_n(i_n) = f_{n'}(i_{n'})$. Cela achève la démonstration du lemme.

Soit L l'extension de $T(\mu_{p^\infty})$ par Z_∞ correspondant aux $f_n(i_n)$. Le reste de cette section est consacrée à prouver que L_χ est libre de rang d sur Λ_χ . Pour cela :

LEMME. - Pour tout entier $n \geq 0$:

- i) l'homomorphisme de $L/\mathfrak{J}_n L$ dans $L/\mathfrak{J}_{n+1} L$ induit par la multiplication par $\omega_{n+1, 1} \times \omega_{n+1, 2}/\omega_{n, 1} \times \omega_{n, 2}$ est injectif,
- ii) on a la suite exacte :

$$0 \rightarrow \mu_{p^\infty}(K_n) \rightarrow Z_\infty / \mathfrak{J}_n Z_\infty \rightarrow L / \mathfrak{J}_n L \rightarrow \mu_{p^\infty}(K_n) \rightarrow 0 ,$$

où les trois flèches de droite sont obtenues en appliquant le foncteur $\cdot \otimes_{\wedge} \wedge / \mathfrak{J}_n$ à la suite exacte :

$$0 \rightarrow Z_\infty \rightarrow L \rightarrow T(\mu_{p^\infty}) \rightarrow 0 ,$$

et où le composé de la flèche de $\mu_{p^\infty}(K_n)$ dans $Z_\infty / \mathfrak{J}_n Z_\infty$ avec l'homomorphisme de $Z_\infty / \mathfrak{J}_n Z_\infty$ dans \widehat{K}_n^* induit par N_{K_∞ / K_n} est l'injection naturelle de $\mu_{p^\infty}(K_n)$ dans \widehat{K}_n^* .

Démonstration. On vérifie facilement que, pour montrer le i) , il suffit de prouver :

$$(II) : \left\{ \begin{array}{l} (1) \text{ Ker} \left(L \xrightarrow{\times \omega_{n+1,1}} L \right) = 0 \\ (2) \text{ Ker} \left(L \xrightarrow{\times \omega_{n+1,2}} L \right) = 0 \\ (3) \text{ Ker} \left(L / \omega_{n+1,1} L \xrightarrow{\times \omega_{n+1,2}} L / \omega_{n+1,1} L \right) = 0 \\ (4) \text{ Ker} \left(L / \omega_{n+1,1} L \xrightarrow{\times \omega_{n,2}} L / \omega_{n+1,1} L \right) = 0 \\ (5) \text{ Ker} \left(L / \omega_{n+1,2} L \xrightarrow{\times \omega_{n+1,1}} L / \omega_{n+1,2} L \right) = 0 \\ (6) \text{ Ker} \left(L / \omega_{n+1,2} L \xrightarrow{\omega_{n,1}} L / \omega_{n+1,2} L \right) = 0 . \end{array} \right.$$

Soit $n \in \mathbb{N}$. D'après la définition de L , on a un homomorphisme de L dans Z_∞ rendant commutatif le diagramme, cf. [3] , chap.IV, §1 :

$$(III) : \begin{array}{ccccccc} 0 & \rightarrow & Z_\infty & \longrightarrow & L & \longrightarrow & T(\mu_{p^\infty}) \longrightarrow 0 \\ & & \parallel \text{Id} & & \downarrow & & \downarrow i_n \\ 0 & \rightarrow & Z_\infty & \xrightarrow{\times \omega_{n,1}} & Z_\infty & \longrightarrow & Z_\infty / \omega_{n,1} Z_\infty \longrightarrow 0 \end{array} .$$

On en déduit, puisque la multiplication par $\omega_{n,1}$ est injective dans Z_∞ , cf. iii) du lemme (5.2) :

$$0 \rightarrow \text{Ker} \left(L \xrightarrow{\times \omega_{n,1}} L \right) \rightarrow T(\mu_{p^\infty}) \rightarrow Z_\infty / \omega_{n,1} Z_\infty \rightarrow L / \omega_{n,1} L \rightarrow T(\mu_{p^\infty}) \rightarrow 0$$

$$\begin{array}{ccccccc} & & \downarrow i_n & & \parallel \text{Id} & & \\ & & Z_\infty / \omega_{n,1} Z_\infty & \xrightarrow{\text{Id}} & Z_\infty / \omega_{n,1} Z_\infty & & \end{array}$$

Comme i_n est injectif, il en résulte que $\text{Ker}(L \xrightarrow{\times \omega_{n,1}} L) = 0$; cela prouve (II),(1).

Soit ℓ un entier ≥ 0 . La multiplication par $\omega_{\ell,2}$ est injective dans le quotient de $Z(F_n(\mu_{p^\infty}))$ par l'image de $T(\mu_{p^\infty})$, puisque, d'après le théorème d'Iwasawa, cf. th. 25 de [1], ce quotient est libre sur l'algèbre des mesures p -adiques sur $\text{Gal}(F_n(\mu_{p^\infty})/F_n)$. La multiplication par $\omega_{\ell,2}$ est donc injective dans le quotient de $Z_\infty/\omega_{n,1}Z_\infty$ par $i_n(T(\mu_{p^\infty}))$. Comme elle l'est aussi dans $T(\mu_{p^\infty})$, il résulte du diagramme ci-dessus que $\text{Ker}(L/\omega_{n,1}L \xrightarrow{\times \omega_{\ell,2}} L/\omega_{n,1}L) = 0$. Cela prouve (II),(3) et (II),(4).

Pour ℓ entier ≥ 0 , on sait, cf. iii) du lemme (5.2), que la multiplication par $\omega_{\ell,2}$ est injective dans Z_∞ . Comme elle l'est aussi dans $T(\mu_{p^\infty})$, on déduit de (III) que $\text{Ker}(L \xrightarrow{\times \omega_{\ell,2}} L) = 0$, et donc on a (II),(2).

Reste à prouver (II),(5), (II),(6) et le ii). Pour cela, comme la multiplication par $\omega_{\ell,2}$ est injective dans $Z_\infty/\omega_{n,1}Z_\infty$ et dans $T(\mu_{p^\infty})$, on déduit de (III) :

$$\begin{array}{ccccccc} 0 & \longrightarrow & Z_\infty/\omega_{\ell,2}Z_\infty & \longrightarrow & L/\omega_{\ell,2}L & \longrightarrow & \mu_{p^{m_0+\ell}} & \longrightarrow & 0 \\ & & \parallel \text{Id} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & Z_\infty/\omega_{\ell,2}Z_\infty & \xrightarrow{\times \omega_{n,1}} & Z_\infty/\omega_{\ell,2}Z_\infty & \longrightarrow & Z_\infty/\omega_{\ell,2}Z_\infty + \omega_{n,1}Z_\infty & \longrightarrow & 0 \end{array}$$

Puisque la multiplication par $\omega_{n,1}$ est injective dans $Z_\infty/\omega_{\ell,2}Z_\infty$, on en déduit :

$$\begin{array}{ccccccc} 0 \longrightarrow & \text{Ker}(L/\omega_{\ell,2}L \xrightarrow{\times \omega_{n,1}} L/\omega_{\ell,2}L) & \longrightarrow & \mu_{p^{m_0+\ell}} & \longrightarrow & Z_\infty/\omega_{\ell,2}Z_\infty + \omega_{n,1}Z_\infty & \longrightarrow & L/\omega_{\ell,2}L + \omega_{n,1}L & \longrightarrow & \mu_{p^{m_0+\ell}} & \longrightarrow & 0 \\ & \searrow & & \downarrow & & \parallel \text{Id} & & & & & & \\ & & & Z_\infty/\omega_{\ell,2}Z_\infty + \omega_{n,1}Z_\infty & \xrightarrow{\text{Id}} & Z_\infty/\omega_{\ell,2}Z_\infty + \omega_{n,1}Z_\infty & & & & & & \end{array}$$

La flèche de $\mu_{\mathbb{P}}^{m_0+\ell}$ dans $Z_{\infty}/\omega_{\ell,2}Z_{\infty} + \omega_{n,1}Z_{\infty}$ se déduit de i_n en prenant le foncteur $\cdot \otimes_{\Lambda} \Lambda/\omega_{\ell,2}\Lambda + \omega_{n,1}\Lambda$. Il en résulte facilement que si on la compose avec l'homomorphisme de $Z_{\infty}/\omega_{\ell,2}Z_{\infty} + \omega_{n,1}Z_{\infty}$ dans $F_n(\mu_{\mathbb{P}}^{\ell+m_0})^*$ induit par la projection, on obtient l'injection naturelle de $\mu_{\mathbb{P}}^{\ell+m_0}$ dans $F_n(\mu_{\mathbb{P}}^{\ell+m_0})^*$. On en déduit que la flèche de $\mu_{\mathbb{P}}^{m_0+\ell}$ dans $Z_{\infty}/\omega_{\ell,2}Z_{\infty} + \omega_{n,1}Z_{\infty}$ est injective. Par suite

$$\text{Ker}(L/\omega_{\ell,2}L \xrightarrow{\times \omega_{n,1}} L/\omega_{\ell,2}L) = 0,$$

et on a la suite exacte :

$$0 \rightarrow \mu_{\mathbb{P}}^{m_0+\ell} \rightarrow Z_{\infty}/\omega_{\ell,2}Z_{\infty} + \omega_{n,1}Z_{\infty} \rightarrow L/\omega_{\ell,2}L + \omega_{n,1}L \rightarrow \mu_{\mathbb{P}}^{m_0+\ell} \rightarrow 0.$$

Cela montre (II) (5), (II) (6) et le ii) et cela achève la démonstration du lemme.

Achevons la démonstration du i) du théorème.

Prouvons tout d'abord que $L_{\infty}/\mathfrak{J}_n L_{\infty}$ est sans torsion, en tant que module sur \mathbb{Z}_p . Soit pour cela $x \in L/\mathfrak{J}_n L$ avec $px = 0$; montrons que $x = 0$. Considérons le diagramme :

$$\begin{array}{ccccccc} L/\mathfrak{J}_n L & \longrightarrow & T(\mu_{\mathbb{P}^{\infty}})/\mathfrak{J}_n T(\mu_{\mathbb{P}^{\infty}}) \simeq \mu_{\mathbb{P}}^{n+m_0} & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ Z_{\infty}/\mathfrak{J}_{n+1} Z_{\infty} & \longrightarrow & L/\mathfrak{J}_{n+1} L \longrightarrow T(\mu_{\mathbb{P}^{\infty}})/\mathfrak{J}_{n+1} T(\mu_{\mathbb{P}^{\infty}}) \simeq \mu_{\mathbb{P}}^{n+m_0+1} & \longrightarrow & 0. \end{array}$$

Les flèches verticales sont induites par la multiplication par $\omega_{n+1,1} \times \omega_{n+1,2} / \omega_{n,1} \times \omega_{n,2}$; en particulier, la flèche de $\mu_{\mathbb{P}}^{n+m_0}$ dans $\mu_{\mathbb{P}}^{n+m_0+1}$ est l'élévation à la puissance p . On voit donc que l'image de x dans $L/\mathfrak{J}_{n+1} L$ appartient à l'image de $Z_{\infty}/\mathfrak{J}_{n+1} Z_{\infty}$ dans $L/\mathfrak{J}_{n+1} L$. L'image de $Z_{\infty}/\mathfrak{J}_{n+1} Z_{\infty}$ dans $L/\mathfrak{J}_{n+1} L$ est sans torsion : cela résulte facilement du diagramme ci-dessous, cf. ii) du lemme précédent :

$$\begin{array}{ccccccc}
 & & & 0 & & & \\
 & & & \downarrow & & & \\
 & & & \mathbb{Z}_p & & & \\
 & & & \downarrow & & & \\
 0 & \longrightarrow & \mu_{p^\infty}(K_{n+1}) & \longrightarrow & Z_\infty/\mathfrak{J}_{n+1}Z_\infty & \longrightarrow & L/\mathfrak{J}_{n+1}L \longrightarrow \mu_{p^\infty}(K_{n+1}) \longrightarrow 0 \\
 & & \searrow & & \downarrow & & \\
 & & & & \widehat{K}_{n+1} & &
 \end{array}$$

On voit alors que l'image de x dans $L/\mathfrak{J}_{n+1}L$ est nulle. Comme, cf. i) du lemme précédent, la flèche de L/\mathfrak{J}_nL dans $L/\mathfrak{J}_{n+1}L$ est injective, c'est que x est nul. Donc L/\mathfrak{J}_nL est sans torsion ; il en est clairement de même de $L_{\bar{\chi}}/\mathfrak{J}_nL_{\bar{\chi}}$.

D'autre part, il résulte immédiatement de la suite exacte du ii) du lemme précédent que $\text{rg}_{A_{\bar{\chi}}} (L_{\bar{\chi}}/\mathfrak{J}_nL_{\bar{\chi}}) = \text{rg}_{A_{\bar{\chi}}} (Z_\infty/\mathfrak{J}_nZ_\infty)$, et donc, cf. lemme (5.5.1), on a $\text{rg}_{A_{\bar{\chi}}} (L_{\bar{\chi}}/\mathfrak{J}_nL_{\bar{\chi}}) = dp^{2n}$. Comme $L_{\bar{\chi}}$ est de type fini en tant que module sur $A_{\bar{\chi}}$, il est séparé et complet pour sa topologie $\mathfrak{M}_{\bar{\chi}}$ -adique. Le lemme (5.4) montre alors qu'il est libre de rang d . Le i) et le ii) du théorème sont complètement démontrés.

Démonstration du iii) du théorème : pour tout $n \in \mathbb{N}$, notons v_n l'homomorphisme de \widehat{K}_n^* dans \mathbb{Z}_p induit par la valuation ; notons e_n l'indice de ramification de K_{n+1} sur K_n et $N_{n+1,n}$ l'homomorphisme N_{K_{n+1}/K_n} . Si U_n est le groupe des unités fondamentales de K_n , on a :

$$\begin{array}{ccccccc}
 0 & \longrightarrow & U_{n+1} & \longrightarrow & \widehat{K}_{n+1}^* & \xrightarrow{v_{n+1}} & \mathbb{Z}_p \longrightarrow 0 \\
 & & \downarrow N_{n+1,n} & & \downarrow N_{n+1,n} & & \downarrow \times p^f/e_n \\
 0 & \longrightarrow & U_n & \longrightarrow & \widehat{K}_n^* & \xrightarrow{v_n} & \mathbb{Z}_p \longrightarrow 0
 \end{array}$$

Avec un argument de compacité facile, on en déduit, passant à la limite projective, la suite exacte :

$$0 \longrightarrow U_\infty \longrightarrow Z_\infty \longrightarrow \varinjlim_{n \in \mathbb{N}} \mathbb{Z}_p \longrightarrow 0 .$$

Si le corps résiduel de K_∞ est infini, on a $e_n = p^{r-1}$ pour tout $n \in \mathbb{N}$ et $\varinjlim_{n \in \mathbb{N}} \mathbb{Z}_p = 0$. D'où $U_\infty = Z_\infty$ et $U_{\infty, \phi} = Z_{\infty, \phi}$ pour tout ϕ .

Si le corps résiduel de K_∞ est fini, on a $e_n = p^r$ pour n grand et $\varinjlim_{n \in \mathbb{N}} \mathbb{Z}_p \simeq \mathbb{Z}_p$. Par suite : $U_{\infty, \phi} = Z_{\infty, \phi}$ pour $\phi \neq \phi_0$, et on a la suite exacte de Λ_{ϕ_0} -modules :

$$0 \longrightarrow U_{\infty, \phi_0} \longrightarrow Z_{\infty, \phi_0} \longrightarrow \mathbb{Z}_p \longrightarrow 0 .$$

Cela achève la démonstration du théorème.

BIBLIOGRAPHIE

- [1] K. IWASAWA, On \mathbb{Z}_p -extensions of algebraic number fields, Ann. of Math. 98 (1973), pp. 246-326.
- [2] S. LANG, Cyclotomic fields, Springer Verlag (1978).
- [3] H. CARTAN et S. EILENBERG, Homological Algebra, Princeton University Press (1956).