

THEORIE DES NOMBRES  
BESANÇON

Années 1979-1980  
et 1980-1981

INTRODUCTION A LA THEORIE D'IWASAWA

Bernard ORIAT

# INTRODUCTION A LA THEORIE D'IWASAWA

---

Bernard ORIAT

Nous donnons ici une approche détaillée du théorème d'Iwasawa ; théorème qui affirme l'existence de  $\lambda, \mu, \nu$  tels que les  $p$ -groupes des classes d'idéaux  $\mathcal{H}_n$  d'une  $\mathbb{Z}_p$ -extension soient, pour  $n$  assez grand, d'ordres  $|\mathcal{H}_n| = p^\mu p^n + \lambda n + \nu$ . Pour cela, nous suivons à peu près l'exposé que Lang réalise de la question dans [4]. Voici quelques titres qui traitent de l'introduction de ce théorème :

[1] Gillard R. Résultats sur les  $\Gamma$ -extensions cyclotomiques, Séminaire de théorie des nombres de Grenoble (1974).

[2] Iwasawa K. On  $\Gamma$ -extensions of algebraic number fields, Bull. Amer. Math. Soc. 65 (1959).

[3] Joly J.R. Etude de l'anneau  $\Lambda = \mathbb{Z}_p[[T]]$ . Structure des  $\Lambda$ -modules de type fini, Séminaire de théorie des nombres de Grenoble (1969).

[4] Lang S. Cyclotomic fields, Springer Verlag (1978).

[5] Serre J.P. Classes des corps cyclotomiques d'après Iwasawa, Séminaire Bourbaki 1958-1959.

C'est dans [2] qu'Iwasawa a énoncé ce théorème. L'introduction de l'anneau  $\Lambda$  est due à Serre [5].

1 - L'anneau  $\Lambda = \mathbb{Z}_p[[X]]$ .

On désigne par  $p$  un nombre premier et par  $\Lambda$  l'anneau  $\mathbb{Z}_p[[X]]$  des séries formelles à coefficients dans  $\mathbb{Z}_p$ . Cet anneau est noethérien. Si  $f$  est un élément de  $\Lambda$ ,  $f = \sum_{n \geq 0} a_n X^n$ ,  $f$  est inversible dans  $\Lambda$  si et seulement si  $f(0) = a_0$  n'est pas congru à 0 modulo  $p$ . Il s'en suit que l'idéal  $(p, X)$  de  $\Lambda$ , engendré par  $p$  et  $X$  est l'unique idéal maximal de  $\Lambda$ .

Algorithme d'Euclide dans  $\Lambda$ .

Proposition 1.1 : Soit  $f = \sum_{i \geq 0} a_i X^i$  un élément de  $\Lambda$ . On suppose qu'il existe un entier  $n$  tel que  $a_i \equiv 0 \pmod{p}$  pour  $0 \leq i \leq n-1$  et  $a_n \not\equiv 0 \pmod{p}$ . Pour tout  $g$  appartenant à  $\Lambda$ , il existe un élément unique  $q$  de  $\Lambda$  et un polynôme unique  $r$  de  $\mathbb{Z}_p[X]$  tels que :

$$\begin{cases} g = fq + r \\ d^0 r \leq n-1 \text{ ou } r = 0. \end{cases}$$

Pour démontrer cette proposition, nous utilisons le lemme :

Lemme 1.2 : Soit  $\tau$  une application  $\mathbb{Z}_p$ -linéaire de  $\Lambda$  dans  $\Lambda$  telle que  $\text{Im } \tau \subset p\Lambda$ . Alors  $\text{id}_\Lambda + \tau$  est un  $\mathbb{Z}_p$ -automorphisme de  $\Lambda$ .

Démonstration : Il est clair que si  $x$  appartient à  $\text{Ker}(\text{id}_\Lambda + \tau)$ , alors  $x$  appartient à  $\bigcap_{i \geq 0} p^i \Lambda = \{0\}$ . Donc  $x = 0$  et  $\text{id}_\Lambda + \tau$  est injectif. Soit  $x$  un élément de  $\Lambda$ . Définissons une suite  $(b_i)_{i \geq 0}$  d'éléments de  $\Lambda$  de la façon suivante : Posons  $b_0 = x$ . On a donc  $b_0 + \tau(b_0) \equiv x \pmod{p}$ . Soit ensuite  $b_1$  défini par  $b_1 = -\tau(b_0)/p$ . On a donc  $b_0 + pb_1 + \tau(b_0 + pb_1) \equiv x \pmod{p^2}$ . Ensuite,  $b_2$  sera défini par  $b_2 = -\tau(b_0 + pb_1)/p$  etc... Posons  $b = b_0 + pb_1 + p^2b_2 + \dots$ . On obtient alors  $b + \tau(b) = x$  et nous avons montré que  $\text{id}_\Lambda + \tau$  est surjectif.

Démontrons maintenant la proposition 1.1 : Pour cela introduisons les applications  $\mathbb{Z}_p$ -linéaires de  $\Lambda$  dans  $\Lambda$  ainsi définies :

$$\alpha : \sum_{i \geq 0} b_i X^i \rightarrow b_0 + b_1 X + \dots + b_{n-1} X^{n-1}.$$

$$\beta : \sum_{i \geq 0} b_i X^i \rightarrow \sum_{i \geq 0} b_{n+i} X^i.$$

L'existence de  $q$  et  $r$  équivaut à l'existence de  $q$  tel que  $\beta(g) = \beta(qf)$ .  
 Mais  $f = \alpha(f) + X^n \beta(f)$  d'où  $\beta(g) = \beta(q\alpha(f)) + \beta(X^n q\beta(f))$ . Soit encore  
 $\beta(g) = \beta(q\alpha(f)) + q\beta(f)$ . Posons  $z = q\beta(f)$ . Comme  $\beta(f)$  est inversible,  
 il reste à résoudre,  $z$  étant l'inconnue :  $\beta(g) = \beta(z\alpha(f)\beta(f)^{-1}) + z$ . Mais  
 $\alpha(f)$  appartient à  $p\Lambda$ . On déduit alors du lemme l'existence de  $z$ .

Définition d'un polynôme distingué : C'est un polynôme unitaire de  $\mathbb{Z}_p[X]$  de la forme  $X^n + p a_{n-1} X^{n-1} + \dots + a_1 p X + a_0 p$  ; avec  $a_i$  dans  $\mathbb{Z}_p$ .

Proposition 1.2 : Si  $f$  est un polynôme distingué, alors l'injection canonique de  $\mathbb{Z}_p[X]$  dans  $\Lambda$  induit un isomorphisme de  $\mathbb{Z}_p$ -modules :  
 $\mathbb{Z}_p[X]/f\mathbb{Z}_p[X] \cong \Lambda/f\Lambda$ .

Démonstration : On considère l'application canonique :  $\mathbb{Z}_p[X] \rightarrow \Lambda/f\Lambda$ .  
 On déduit de l'algorithme d'Euclide dans  $\Lambda$ , que cette application est surjective. Si maintenant  $h$  appartient à  $\mathbb{Z}_p[X] \cap f\Lambda$ , divisons  $h$  par  $f$  dans  $\mathbb{Z}_p[X]$ . Nous obtenons  $h = fq + h_1$  avec  $d^0 h_1 \leq d^0 f - 1$ . Le reste  $h_1$  appartient à  $f\Lambda$ . On déduit alors de l'unicité de l'algorithme d'Euclide que  $h_1 = 0$ .  
 Donc le noyau de cette application est  $f\mathbb{Z}_p[X]$ .

Définition du degré de Weierstrass : Si  $f$  est un élément de  $\Lambda$ ,  
 $f = \sum_{n \geq 0} a_n X^n$ , on appelle degré de Weierstrass de  $f$ , noté  $\deg_W(f)$  le plus petit entier  $i$  tel que  $a_i \not\equiv 0 \pmod{p}$ . Lorsque  $f$  appartient à  $p\Lambda$ , on posera  $\deg_W(f) = +\infty$ .

Proposition 1.3 : Soit  $f$  un élément de  $\Lambda$ , n'appartenant pas à  $p\Lambda$ . Posons  $n = \deg_W(f)$ . Il existe un polynôme distingué  $h$  de degré  $n$  et un élément inversible  $u$  de  $\Lambda$  tels que  $f = uh$ .

Démonstration : Posons  $f = \sum_{m \geq 0} a_m X^m$ . On a donc  $a_0 \equiv 0 \pmod{p}, \dots, a_{n-1} \equiv 0 \pmod{p}$  et  $a_n \not\equiv 0 \pmod{p}$ . Utilisons l'algorithme d'Euclide : il existe  $q$  et  $r$  tels que  $X^n = fq + r$  avec  $r \in \mathbb{Z}_p[X]$  et  $\deg r \leq n-1$ . En réduisant modulo  $p$ , il reste  $r \equiv 0 \pmod{p}$  et  $X^n - r$  est un polynôme distingué de degré  $n$ . D'autre part, si  $q = \sum_{i \geq 0} b_i X^i$ , nous avons  $1 = a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0$  et nous obtenons  $a_n b_0 \equiv 1 \pmod{p}$ . Donc  $q$  est un élément inversible de  $\Lambda$  et on peut écrire  $f = (X^n - r) q^{-1}$ .

## 2 - Structure des $\Lambda$ -modules de type fini.

La notion de base employée pour préciser cette structure est la notion de quasi-isomorphisme :

Définition d'un quasi-isomorphisme de  $\Lambda$ -modules : Soient  $V$  et  $W$  deux  $\Lambda$ -modules. Un quasi-isomorphisme  $\alpha$  de  $V$  dans  $W$  est une application  $\Lambda$ -linéaire de  $V$  dans  $W$ , dont le noyau et le conoyau sont finis (Rappelons que  $\text{Coker } \alpha = W/\text{Im } \alpha$ ).

Remarques : La somme directe de deux quasi-isomorphismes est un quasi-isomorphisme. Le composé de deux quasi-isomorphismes est aussi un quasi-isomorphisme. Mais l'existence d'un quasi-isomorphisme de  $V$  dans  $W$  n'implique pas l'existence d'un quasi-isomorphisme de  $W$  dans  $V$  : Considérons en effet l'idéal de  $\Lambda$  engendré par  $p$  et  $X$ , noté  $(p, X)$ , et la suite exacte :

$$0 \rightarrow (p, X) \rightarrow \Lambda \rightarrow \mathbb{F}_p \rightarrow 0.$$

L'injection canonique de  $(p, X)$  dans  $\Lambda$  est donc un quasi-isomorphisme. Mais il n'existe pas de quasi-isomorphisme de  $\Lambda$  dans  $(p, X)$  : soit  $\theta$  une application  $\Lambda$ -linéaire de  $\Lambda$  dans  $(p, X)$ . L'image de 1 par  $\theta$  a un degré de Weierstrass supérieur à 1. Si ce degré est fini, on peut l'écrire sous la forme  $uh$ ,  $u$  élément inversible et  $h$  polynôme distingué de degré supérieur à 1 (Proposition 1.3). On a alors  $\text{Im } \theta = h\Lambda$  et  $(\Lambda : h\Lambda) = (\mathbb{Z}_p[X] : h\mathbb{Z}_p[X])$

est infini. Donc  $\text{Coker } \theta = (p, X)/h\Lambda$  est infini. Si l'image de 1 par  $\theta$  appartient à  $p\Lambda$ , on a le même résultat.

La méthode que nous exposons ci-après s'inspire de la méthode classique de détermination de la structure des modules sur un anneau principal.

Définition de  $\hat{R}$  : Soit  $R$  une matrice à coefficients dans  $\Lambda$ . Soit  $n$  le nombre de ses colonnes. Ses lignes sont des éléments de  $\Lambda^n$  et on note  $\hat{R}$  le sous- $\Lambda$ -module engendré par les lignes de  $R$ . On considère le  $\Lambda$ -module  $\Lambda^n/\hat{R}$ . Il est de type fini. Réciproquement on a la proposition :

Proposition 2.1 : Si  $M$  est un  $\Lambda$ -module de type fini, il existe un entier  $n$  et une matrice  $R$  à  $n$  colonnes telle que  $M$  soit  $\Lambda$ -isomorphe à  $\Lambda^n/\hat{R}$ .

Démonstration : Soit  $(u_i)_{1 \leq i \leq n}$  un système de générateurs de  $M$ . Faisons correspondre à la suite  $(\lambda_1, \dots, \lambda_n)$  de  $\Lambda^n$  l'élément  $\lambda_1 u_1 + \dots + \lambda_n u_n$  de  $M$ . Le noyau de cette application  $\Lambda$ -linéaire est de type fini, puisque  $\Lambda$  est noethérien. Un système de générateurs de ce noyau forme les lignes de la matrice  $R$  cherchée.

Opérations élémentaires : Soit  $R$  une matrice, à  $n$  colonnes, à coefficients dans  $\Lambda$ . Une opération élémentaire sur les lignes de  $R$  est :

ou l'échange de deux lignes,

ou l'addition à une ligne d'une combinaison  $\Lambda$ -linéaire des autres lignes,

ou la multiplication d'une ligne par un élément inversible de  $\Lambda$ . Il est clair que si  $R'$  est déduite de  $R$  par une opération élémentaire sur les lignes, alors  $\hat{R} = \hat{R}'$  et  $\Lambda^n/\hat{R} = \Lambda^n/\hat{R}'$ .

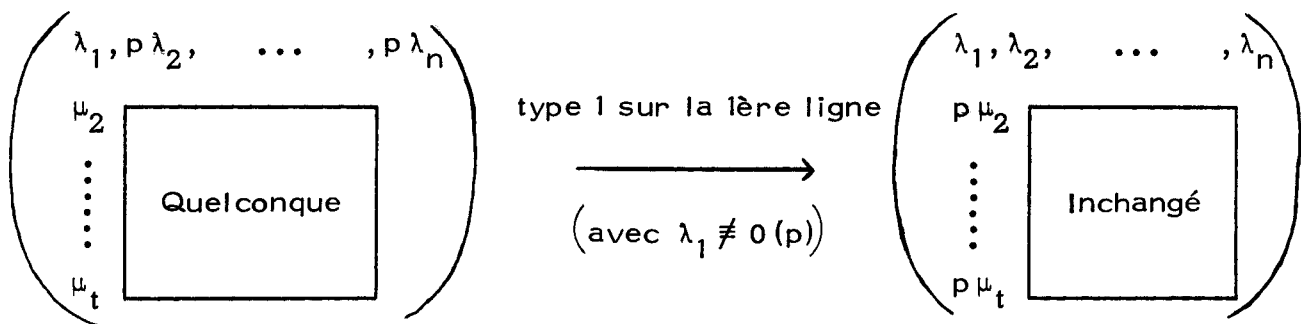
Une opération élémentaire sur les colonnes se définit de la même façon. Si  $R'$  est déduite de  $R$  par une opération élémentaire sur les colonnes, alors  $\Lambda^n/\hat{R}'$  est isomorphe à  $\Lambda^n/\hat{R}$ .

En plus de ces opérations élémentaires utilisées dans la théorie classique des modules sur un anneau principal, nous allons introduire d'autres opérations dites "admissibles" :

On désigne par  $R$  une matrice à  $n$  colonnes et  $t$  lignes, à coefficients dans  $\Lambda$ . Posons  $R = (a_{ij})$ .

Définition d'une opération admissible de type 1 : Pour réaliser une telle opération sur la  $i^{\text{ème}}$  ligne, il faut que  $a_{ii} \not\equiv 0 \pmod{p}$  et  $a_{ij} \equiv 0 \pmod{p}$  pour  $j \neq i$ . Cette opération consiste à diviser  $a_{ij}$  pour  $j \neq i$  par  $p$  et à multiplier  $a_{ki}$ , pour  $k \neq i$ , par  $p$ . L'élément  $a_{ii}$  reste invariant.

En résumé :



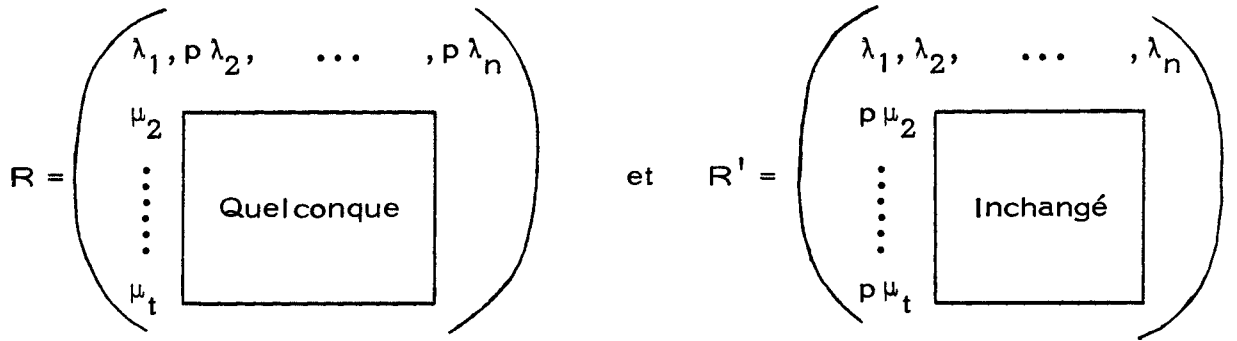
Proposition 2.2 : On suppose que  $R$  vérifie l'hypothèse permettant de réaliser une opération admissible de type 1 sur l'une de ses lignes. Soit  $R'$  la matrice déduite de  $R$  par cette opération. Alors il existe un quasi-isomorphisme de  $\Lambda^n/\hat{R}$  dans  $\Lambda^n/\hat{R}'$ .

Démontrons tout d'abord le lemme suivant :

Lemme 2.3 : Soit  $M$  un  $\Lambda$ -module de type fini, annulé par une puissance de  $p$  et par un polynôme distingué. Alors  $M$  est fini.

Démonstration : Soit  $p^k$  la puissance de  $p$  qui annule  $M$  et  $\lambda$  le polynôme distingué qui annule  $M$ . Soit  $\{u_1, \dots, u_n\}$  un système de générateurs de  $M$ . On déduit de l'application  $(a_1, \dots, a_n) \rightarrow a_1 u_1 + \dots + a_n u_n$  de  $\Lambda^n$  dans  $M$ , une application  $\Lambda$ -linéaire surjective  $\xrightarrow{\text{de}} (\Lambda/p^k \Lambda + \lambda \Lambda)^n$  sur  $M$ .  
 Mais  $\Lambda/p^k \Lambda + \lambda \Lambda \cong (\Lambda/\lambda \Lambda) / ((p^k \Lambda + \lambda \Lambda)/\lambda \Lambda) = (\Lambda/\lambda \Lambda) / p^k (\Lambda/\lambda \Lambda)$   
 $\cong (\mathbb{Z}_p[X]/\lambda \mathbb{Z}_p[X]) / p^k (\mathbb{Z}_p[X]/\lambda \mathbb{Z}_p[X])$  est fini.

Démonstration de la proposition : Reprenons la notation introduite plus haut :



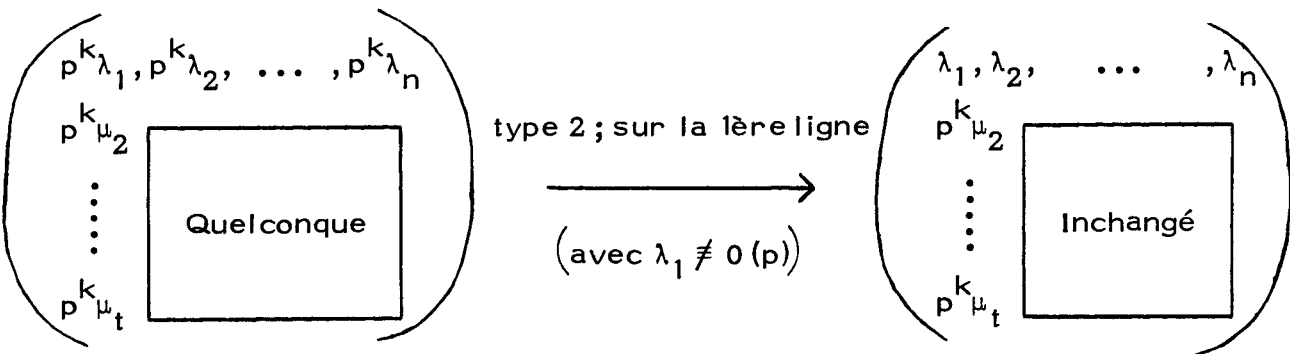
Considérons l'application de  $\Lambda^n$  dans  $\Lambda^n$  qui fait correspondre à  $(a_1, \dots, a_n)$  l'élément  $(pa_1, a_2, \dots, a_n)$  de  $\Lambda^n$ . Il est clair que cette application envoie  $\hat{R}$  dans  $\hat{R}'$ . On en déduit donc une application  $\Lambda$ -linéaire  $\theta$  de  $\Lambda^n/\hat{R}$  dans  $\Lambda^n/\hat{R}'$  définie par

$$(a_1, \dots, a_n) + \hat{R} \mapsto (pa_1, a_2, \dots, a_n) + \hat{R}'$$

Son image est  $[(p\Lambda \times \Lambda \times \dots \times \Lambda) + \hat{R}']/\hat{R}'$  et son conoyau est  $\Lambda^n/(p\Lambda \times \Lambda \times \dots \times \Lambda) + \hat{R}'$ .

Ce conoyau est annulé par  $p$  et par  $\lambda_1$ . Donc d'après le lemme, il est fini. D'autre part, on peut vérifier que son noyau est réduit 0. Donc  $\theta$  un quasi-isomorphisme.

Définition d'une opération admissible de type 2 : Pour réaliser une telle opération sur la  $i^{\text{ème}}$  ligne, il est nécessaire que  $a_{ij} \equiv 0 \pmod{p^k}$  pour tout  $j$ ,  $a_{ki} \equiv 0 \pmod{p^k}$  pour tout  $k$  et enfin  $a_{ii} \not\equiv 0 \pmod{p^{k+1}}$ . Cette opération consiste alors à diviser les termes de la  $i^{\text{ème}}$  ligne par  $p^k$ . Soit en résumé :



Proposition 2.3 : Soit  $R$  une matrice à coefficients dans  $\Lambda$ , pouvant subir une opération de type 2 sur la  $i^{\text{ème}}$  ligne ; c'est-à-dire qu'il existe un entier  $k$  tel que  $a_{ij} \equiv 0 \pmod{p^k}$  pour tout  $j$  ;  $a_{ki} \equiv 0 \pmod{p^k}$  pour tout  $k$  et



$a_{ij} \not\equiv 0 \pmod{p^{k+1}}$ . Soit  $R'$  la matrice déduite de  $R$  par l'opération admissible de type 2 sur la  $i^{\text{ème}}$  ligne. Alors il existe un quasi-isomorphisme de  $\Lambda^n/\hat{R}$  dans  $(\Lambda^n/\hat{R}') \oplus (\Lambda/p^k\Lambda)$ .

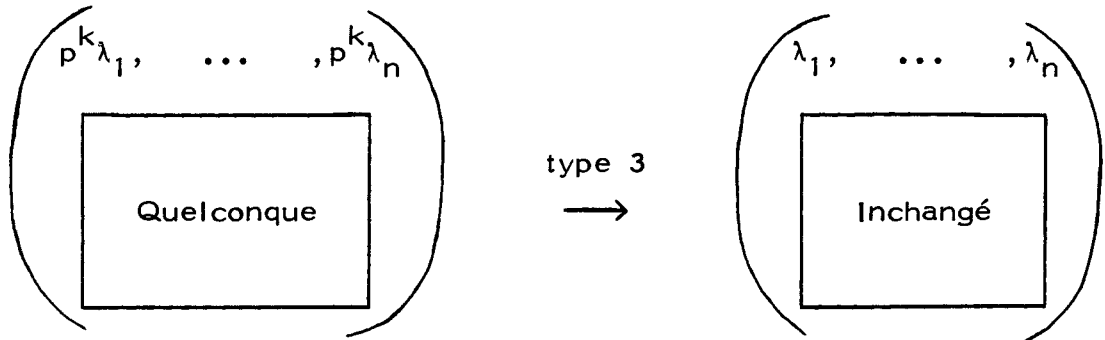
Démonstration : Reprenons la notation simplifiée : (avec  $\lambda_1 \not\equiv 0 \pmod{p}$ )

$$R = \left( \begin{array}{c} p^k \lambda_1, p^k \lambda_2, \dots, p^k \lambda_n \\ p^k \mu_2 \\ \vdots \\ p^k \mu_t \end{array} \begin{array}{c} \boxed{\text{Quelconque}} \end{array} \right) \quad \text{et} \quad R' = \left( \begin{array}{c} \lambda_1, \lambda_2, \dots, \lambda_n \\ p^k \mu_2 \\ \vdots \\ p^k \mu_t \end{array} \begin{array}{c} \boxed{\text{Inchangé}} \end{array} \right)$$

Considérons l'application de  $\Lambda^n$  dans  $(\Lambda^n/\hat{R}') \oplus (\Lambda/p^k\Lambda)$  qui fait correspondre à  $(a_1, \dots, a_n)$  l'élément  $((a_1, \dots, a_n) + \hat{R}', a_1 + p^k\Lambda)$ . Cette application envoie  $\hat{R}$  dans 0. On en déduit donc une application  $\theta$   $\Lambda$ -linéaire de  $\Lambda^n/\hat{R}$  dans  $(\Lambda^n/\hat{R}') \oplus (\Lambda/p^k\Lambda)$ . Elle est injective. Pour montrer que le conoyau de cette application est fini, nous montrons qu'il est annulé par  $p^k$  et  $\lambda_1$ . Soit  $((b_1, \dots, b_n) + \hat{R}', b_0 + p^k\Lambda)$  un élément de  $(\Lambda^n/\hat{R}') \oplus (\Lambda/p^k\Lambda)$ . Si on le multiplie par  $p^k$ , alors on constate qu'il est l'image par  $\theta$  de  $(p^k b_1, \dots, p^k b_n) + \hat{R}$ . Si on le multiplie par  $\lambda_1$ , on peut l'écrire :  $[\lambda_1(b_1, \dots, b_n) + \hat{R}', \lambda_1 b_0 + p^k\Lambda] = [(\lambda_1 b_0, \dots, \lambda_1 b_n - \lambda_n(b_1 - b_0)) + \hat{R}', \lambda_1 b_0 + p^k\Lambda]$  et il apparaît ainsi comme un élément de  $\text{Im } \theta$ . Ceci termine la démonstration.

Définition d'une opération admissible de type 3 : Pour pouvoir réaliser une telle opération sur la  $i^{\text{ème}}$  ligne de la matrice  $R$ , il faut que les termes de cette  $i^{\text{ème}}$  ligne soient tous divisibles par  $p^k$ , c'est-à-dire :  $a_{ij} \equiv 0 \pmod{p^k}$  pour tout  $j$  et qu'il existe un élément  $\lambda$  de  $\Lambda$ , non divisible par  $p$ , tel que  $(\lambda a_{i1} p^{-k}, \dots, \lambda a_{in} p^{-k})$  appartienne à  $\hat{R}$ . L'opération admissible de type 3 sur la  $i^{\text{ème}}$  ligne consiste à diviser les éléments de cette ligne par  $p^k$ .

En résumé, voici une opération de type 3 sur la première ligne  
 (sous l'hypothèse : il existe  $\lambda \in \Lambda$ ,  $\lambda \neq 0 \pmod{p}$  tel que  
 $(\lambda \lambda_1, \dots, \lambda \lambda_n) \in \hat{R}$ ) :



Proposition 2.4 : Soit  $R$  une matrice susceptible de subir une opération admissible de type 3. Soit  $R'$  la matrice déduite de  $R$  par cette opération. Alors il existe un quasi-isomorphisme de  $\Lambda^n/\hat{R}$  dans  $\Lambda^n/\hat{R}'$ .

Démonstration : Il suffit de considérer l'application naturelle de  $\Lambda^n/\hat{R}$  dans  $\Lambda^n/\hat{R}'$  déduite de l'inclusion  $\hat{R} \subset \hat{R}'$ . Elle est surjective. Son noyau est  $\hat{R}'/\hat{R}$ . Ce  $\Lambda$ -module est annihilé par  $\lambda$  et par  $p^k$ . Il est donc fini, d'après le lemme énoncé plus haut.

Nous pouvons maintenant énoncer le théorème essentiel :

Théorème 2.5 : Soit  $R$  une matrice à coefficients dans  $\Lambda$ . Il existe une suite de polynômes distingués  $\lambda_1, \dots, \lambda_r$  et une suite d'opérations élémentaires ou admissibles permettant de transformer la matrice  $R$  en une matrice  $R'$  de la forme :

$$R' = \begin{pmatrix} \lambda_1 & 0 \dots 0 & 0 \dots 0 \\ 0 & \lambda_2 & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 \dots \lambda_r & 0 \dots 0 \\ 0 & 0 \dots 0 & 0 \dots 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 \dots 0 & 0 \dots 0 \end{pmatrix}$$

La démonstration de ce théorème va utiliser la définition suivante :

Définition de  $\text{deg}_k R$  : Soit toujours  $R$  une matrice à coefficients

dans  $\Lambda$  et  $k$  un entier inférieur à son nombre de lignes et de colonnes. On considère l'ensemble de toutes les matrices qui peuvent être déduites de  $R$  par des suites d'opérations élémentaires ou admissibles, laissant invariant les  $(k-1)$  premières lignes. Si  $(a_{ij})$  est une telle matrice, on s'intéresse au minimum :  $\min_{\substack{i \geq k \\ j \geq k}} \text{deg}_W(a_{ij})$  ;  $i$  et  $j$  étant supérieurs à  $k$ .

On désigne par  $\text{deg}_k R$ , le plus petit de ces minimum,  $(a_{ij})$  parcourant l'ensemble des matrices considéré.

Remarque : Si  $R'$  est déduite de  $R$  par une opération élémentaire ou admissible laissant invariant les  $(k-1)$  premières lignes, alors  $\text{deg}_k R \leq \text{deg}_k R'$ .

En effet, l'ensemble des matrices qui peuvent être déduites de  $R'$  par des opérations élémentaires ou admissibles laissant invariant les  $(k-1)$  premières lignes est inclus dans l'ensemble des matrices qui peuvent être déduites de  $R$  de la même façon. D'où cette inégalité.

Pour démontrer le théorème 2.5, nous démontrons d'abord cette proposition :

Proposition 2.6 : Soit  $R$  une matrice à coefficients dans  $\Lambda$ . On peut, à l'aide d'une suite d'opérations élémentaires ou admissibles, transformer  $R$  en une matrice  $R'$  de la forme

$$R' = \begin{pmatrix} \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_r \end{pmatrix} & \begin{pmatrix} \\ \\ 0 \\ \\ \end{pmatrix} \\ \begin{pmatrix} \\ \\ \\ \\ \end{pmatrix} \times \begin{pmatrix} \\ \\ \\ \\ \end{pmatrix} & \begin{pmatrix} \\ \\ 0 \\ \\ \end{pmatrix} \end{pmatrix}$$

où  $\lambda_1, \dots, \lambda_r$  sont des polynômes distingués vérifiant les conditions :  
 Pour  $1 \leq \ell \leq r$ ,  $d^\circ \lambda_\ell = \deg_\ell R'$ .

Pour démontrer cette proposition, nous procédons par récurrence au moyen de la proposition suivante :

Proposition 2.7 : Soit  $R$  une matrice à coefficients dans  $\Lambda$  de la forme

$$R = \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_{r-1} \end{pmatrix} & \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\ \begin{pmatrix} \vdots \\ \vdots \\ \vdots \end{pmatrix} & \begin{pmatrix} \vdots \\ \vdots \\ \vdots \end{pmatrix} \\ X & Y \end{pmatrix}$$

où  $\lambda_1, \dots, \lambda_{r-1}$  sont des polynômes distingués tels que pour  $1 \leq \ell \leq r-1$ ,  $d^\circ \lambda_\ell = \deg_\ell R$ . Si le bloc  $(Y)$  n'est ni nul, ni vide, alors il existe une suite d'opérations élémentaires ou admissibles permettant de transformer  $R$  en une matrice  $R'$  de la forme

$$R' = \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_{r-1} \\ & & & \lambda_r \end{pmatrix} & \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} \vdots \\ \vdots \\ \vdots \\ \vdots \end{pmatrix} & \begin{pmatrix} \vdots \\ \vdots \\ \vdots \\ \vdots \end{pmatrix} \\ X' & Y' \end{pmatrix}$$

où  $\lambda_r$  est encore un polynôme distingué et où les polynômes  $\lambda_1, \dots, \lambda_r$  vérifient encore les conditions : pour  $1 \leq \ell \leq r$ ,  $d^0 \lambda_\ell = \deg_\ell R^1$ .

Démonstration : Posons  $R = (\lambda_{ij})$  et convenons de noter  $\lambda_i$  pour  $\lambda_{ij}$ . A l'aide d'opérations admissibles de type 1 sur les lignes  $1, 2, \dots, r-1$ , on peut multiplier les éléments de  $X$  par  $p$  autant de fois que l'on veut, sans modifier les  $r-1$  premières lignes de  $R$ . Une permutation de colonnes d'indices supérieurs à  $r$  suivie d'une opération admissible de type 2 sur la  $r^{\text{ème}}$  ligne peuvent alors (puisque  $Y \neq (0)$ ) faire apparaître un  $\lambda_r \neq 0 \pmod{p}$ . Nous avons donc vérifié ainsi que  $\deg_r R \neq \infty$ .

Il existe donc une suite de transformations admissibles et élémentaires laissant invariant les  $r-1$  premières lignes et transformant la matrice  $R$  en une matrice  $R^1 = (\lambda'_{ij})$  telle que :  $\deg_r R^1 = \deg_W \lambda'_{ij}$  pour un  $i$  et un  $j$  supérieur à  $r$ . Effectuant une permutation de lignes et colonnes, nous pouvons supposer  $i = j = r$ . Multipliant la  $r^{\text{ème}}$  colonne par une unité adéquate, nous pouvons supposer que  $\lambda'_r = \lambda'_{rr}$  est un polynôme distingué. Il vérifie  $d^0 \lambda'_r = \deg_r R^1$ . Des opérations élémentaires laissant invariant les  $r-1$  premières lignes permettent, en utilisant l'algorithme d'Euclide, de faire apparaître sur la  $r^{\text{ème}}$  ligne des polynômes  $\lambda'_{rj}$  tels que :  $d^0 \lambda'_{rj} < d^0 \lambda'_r$  pour  $r \neq j$  et  $d^0 \lambda'_{rj} < d^0 \lambda_j$  pour  $j < r$ . (Il est clair que  $\lambda_j = \lambda'_j$  pour  $1 \leq j \leq r-1$ , puisque les  $r-1$  premières lignes n'ont pas été modifiées).

Il reste à montrer que la matrice  $R^1$  vérifie les conditions annoncées. Si  $1 \leq \ell \leq r-1$ , on déduit de la remarque faite plus haut que :

$d^0 \lambda_\ell = \deg_\ell R \leq \deg_\ell R^1 \leq d^0 \lambda'_\ell = d^0 \lambda_\ell$ . Donc  $d^0 \lambda_\ell = \deg_\ell R^1$ . De même, par définition de  $\lambda'_r$ , on a  $d^0 \lambda'_r = \deg_r R$ . Donc  $d^0 \lambda'_r = \deg_r R^1$ .

Montrons maintenant que  $\lambda'_{ri} = 0$  pour  $i \geq r+1$ . La condition  $d^0 \lambda'_{ri} < d^0 \lambda'_r$  et la définition de  $\lambda'_r$  :  $d^0 \lambda'_r = \deg_r R = \deg_r R^1$ , montre que  $\deg_W (\lambda'_{ri}) = +\infty$ , ou en d'autres termes  $\lambda'_{ri} \equiv 0 \pmod{p}$ . Supposons que les  $\lambda'_{ri}$ ,  $i \geq r+1$  ne soient pas tous nuls et soit  $k$  tel que  $p^k$  ne divise pas ces  $\lambda'_{ri}$ . En utilisant des opérations de type 1 sur les lignes  $1, 2, \dots, r-1$ , on peut multiplier  $\lambda'_{rj}$  pour  $1 \leq j \leq r-1$  par  $p$  autant de fois que l'on veut, de

façon à avoir  $\lambda'_{rj} \equiv 0 \pmod{p^k}$ . Utilisant encore l'opération de type 1 sur la  $r^{\text{ème}}$  ligne, on fera apparaître un  $\lambda''_{ri}$ ,  $i \geq r+1$ , tel que  $\deg_W(\lambda''_{ri}) < d^0 \lambda_r$ . Contradiction.

Montrons enfin que  $\lambda'_{ri} = 0$  pour  $1 \leq i \leq r-1$ . Nous avons  $d^0 \lambda'_{ri} < d^0 \lambda_i$ . Si pour  $1 \leq i \leq r-1$ , il existait un  $\lambda'_{ri} \neq 0$ , il devrait vérifier  $\lambda'_{ri} \equiv 0 \pmod{p}$ , sinon il contredirait la condition  $\deg_i R' = d^0 \lambda_i$ . Mais en effectuant l'opération élémentaire de type 1 sur la  $r^{\text{ème}}$  ligne, autant de fois que nécessaire, on peut faire apparaître un  $\lambda''_{ri}$ , tel que  $\deg_W \lambda''_{ri} < d^0 \lambda_i$ . Contradiction.

Ainsi la matrice  $R'$  a bien la forme annoncée. Ceci termine la démonstration de la propriété 2.7. La proposition 2.6 s'en déduit immédiatement.

Pour terminer la démonstration du théorème, nous utilisons la proposition suivante :

Proposition 2.8 : Soit  $R$  une matrice à coefficients dans  $\Lambda$  de la forme

$$R = \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \dots & \\ 0 & & \lambda_r \end{pmatrix} & \begin{pmatrix} 0 \\ \\ \\ \end{pmatrix} \\ \begin{pmatrix} \\ \\ \\ \end{pmatrix} & \begin{pmatrix} \\ \\ 0 \\ \end{pmatrix} \end{pmatrix}$$

$\lambda_1, \dots, \lambda_r$  étant des polynômes distingués tels que pour  $1 \leq \ell \leq r$ ,

$d^0 \lambda_\ell = \deg_\ell R$ . Alors on peut déduire de  $R$ , à l'aide d'opérations élémentaires, la matrice :

$$R' = \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \dots & \\ 0 & & \lambda_r \end{pmatrix} & \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} & \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \end{pmatrix}$$

Démonstration : Soit  $R = (\lambda_{ij})$  la matrice donnée. Posons  $\lambda_i = \lambda_{ii}$ .

Utilisant des opérations élémentaires et l'algorithme d'Euclide, on peut transformer  $R$  en  $R' = (\lambda'_{ij})$ , où  $\lambda'_{ij}$ , pour  $i > r$ , sont des polynômes tels que  $d^0 \lambda'_{ij} < d^0 \lambda_j$  pour  $i > r$  et  $1 \leq j \leq r$ . Comme ces opérations laissent invariantes les  $r$  premières lignes, et utilisant la remarque, on a donc encore  $d^0 \lambda_i = \deg_i R'$  pour  $1 \leq i \leq r$ .

Il reste à montrer que si  $i > r$ , alors  $\lambda'_{ij} = 0$ . Supposons qu'il n'en soit pas ainsi et que  $\lambda'_{ij} \neq 0$ . La condition  $d^0 \lambda'_\ell = \deg_\ell R'$  et la condition  $d^0 \lambda'_{i\ell} < d^0 \lambda'_\ell$  implique  $\lambda'_{i\ell} \equiv 0 \pmod{p}$ . Posons donc  $\lambda'_{ik} = p \lambda''_{ik}$  et la  $i^{\text{ème}}$  ligne de  $R'$  est de la forme :

$$(p \lambda''_{i1}, p \lambda''_{i2}, \dots, p \lambda''_{in}).$$

D'autre part, posons  $\lambda = \lambda_1 \lambda_2 \dots \lambda_r$ . Il s'agit là d'un polynôme distingué et  $(\lambda, 0, \dots, 0)$ ,  $(0, \lambda, 0, \dots, 0)$ , etc..., appartiennent à  $\hat{R}'$ . Donc  $(\lambda \lambda''_{i1}, \dots, \lambda \lambda''_{in})$  appartient à  $\hat{R}'$ . Utilisons alors l'opération admissible de type 3 sur la  $i^{\text{ème}}$  ligne. On peut donc remplacer dans  $\hat{R}'$  la  $i^{\text{ème}}$  ligne par

$$(\lambda''_{i1}, \lambda''_{i2}, \dots, \lambda''_{in}) \text{ sans changer les conditions } d^0 \lambda'_\ell = \deg_\ell R'.$$

En répétant cette opération le nombre de fois qu'il faut, on fait apparaître un terme d'indices  $ij$  qui contredit la condition  $d^0 \lambda_j = \deg_j$ .

Ceci termine la démonstration de la proposition 2.8 et du théorème 2.5. Des résultats énoncés dans ce paragraphe, nous déduisons immédiatement :

Théorème 2.9 : Soit  $V$  un  $\Lambda$ -module de type fini. Il existe un entier  $s$ , des polynômes distingués  $\lambda_1, \dots, \lambda_r$ , des entiers  $m_1, \dots, m_t$  et un quasi-isomorphisme de  $V$  dans  $\Lambda^s \oplus \left( \bigoplus_i (\Lambda/\lambda_i \Lambda) \right) \oplus \left( \bigoplus_i (\Lambda/p^{m_i} \Lambda) \right)$ .

Remarque : Si  $\lambda_1$  et  $\lambda_2$  sont deux polynômes distingués premiers entre eux,  $\Lambda/\lambda_1 \lambda_2 \Lambda$  est quasi-isomorphe à  $\Lambda/\lambda_1 \Lambda \oplus \Lambda/\lambda_2 \Lambda$ . Par suite il est possible dans le théorème précédent d'imposer de plus à  $\lambda_1, \dots, \lambda_r$  d'être des puissances de polynômes distingués irréductibles. Avec cette condition supplémentaire, les paramètres  $\lambda_1, \dots, \lambda_r, m_1, \dots, m_t$  et  $s$  sont uniques. La démonstration de cette unicité s'appuie sur la notion de dimension d'un module libre sur un anneau principal (on utilise ici les anneaux  $\mathbb{Z}_p$  et  $\mathbb{F}_p[[X]]$ ) et sur les lemmes suivants :

Lemme : Soient  $V$  et  $V'$  deux  $\Lambda$ -modules,  $T$  et  $T'$  leurs sous-modules de torsion respectifs. Si  $V$  est quasi-isomorphe à  $V'$ , alors  $T$  est quasi-isomorphe à  $T'$  et  $V/T$  est quasi-isomorphe à  $V'/T'$ .

Lemme : Soient  $V$  et  $V'$  deux  $\Lambda$ -modules et  $\lambda$  un élément quelconque  $\Lambda$ . Si  $V$  est quasi-isomorphe à  $V'$ , alors  $\lambda V$  est quasi-isomorphe à  $\lambda V'$  et  $V/\lambda V$  est quasi-isomorphe à  $V'/\lambda V'$ .

### 3 - Module d'Iwasawa.

Définition des polynômes  $h_n$  et  $g_n$  : Pour tout entier  $n$ , on pose

$h_n = (1+X)^{p^n} - 1$  et  $g_n = h_n/X = 1 + (1+X) + \dots + (1+X)^{p^n - 1}$ . Ces polynômes sont des polynômes distingués de  $\mathbb{Z}_p[X]$ . On a  $g_0 = 1$  et  $g_{n+1} = g_n [1 + (1+X)^{p^n} + \dots + (1+X)^{(p-1)p^n}]$ .



Définition d'un module d'Iwasawa : Soit  $V$  un  $\Lambda$ -module. Soit  $\tau_1, \dots, \tau_s$  des éléments en nombre fini de  $V$ . On dit que  $V$  est un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa si  $V$  est un  $\Lambda$ -module de type fini et si pour tout entier  $n$  le module quotient  $V/g_n(XV + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s)$  est fini.

Cas particulier : Un 0-module d'Iwasawa est un  $\Lambda$ -module  $V$  de type fini tel que  $V/((1+X)^{p^n} - 1)V$  soit fini pour tout  $n$ .

Proposition 3.1 : Soit  $V$  un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. Soit  $\alpha$  une application  $\Lambda$ -linéaire de  $V$  dans  $W$ . On suppose que le conoyau de  $\alpha$  est fini. Alors  $W$  est un  $(\alpha(\tau_1), \dots, \alpha(\tau_s))$ -module d'Iwasawa.

Démonstration : Puisque  $V$  est de type fini et que  $(W : \alpha(V))$  est fini, alors  $W$  est aussi de type fini. Posons  $U = XV + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s$ . On déduit de  $\alpha$  une suite exacte :

$$V/g_n U \longrightarrow \alpha(V)/\alpha(g_n U) \longrightarrow 0.$$

De plus, on a  $\alpha(g_n U) = g_n \alpha(U)$ . Donc  $(\alpha(V) : g_n \alpha(U))$  est fini. Donc  $(W : g_n \alpha(U))$  est fini. Constatons enfin que

$$\alpha(U) = \alpha[XV + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s] = X\alpha(V) + \mathbb{Z}_p \alpha(\tau_1) + \dots + \mathbb{Z}_p \alpha(\tau_s).$$

Donc  $\alpha(U) \subset XW + \mathbb{Z}_p \alpha(\tau_1) + \dots + \mathbb{Z}_p \alpha(\tau_s)$ . Ceci montre que  $W/g_n(XW + \mathbb{Z}_p \alpha(\tau_1) + \dots + \mathbb{Z}_p \alpha(\tau_s))$  est fini.

Lemme 3.2 : Soient  $V$  un  $\Lambda$ -module et  $U$  un sous-module de  $V$ . On suppose que  $V/U$  est fini. Alors il existe un entier  $n_0$  et une constante entière  $c$  tels que pour  $n \geq n_0$ , on ait  $(g_n V : g_n U) = p^c$ .

Démonstration : A partir de la multiplication par  $g_n$  on forme une suite exacte  $V/U \longrightarrow g_n V/g_n U \longrightarrow 0$ . Elle montre que  $(g_n V : g_n U)$  est fini. De plus  $g_{n+1}$  est un multiple de  $g_n$ . On peut donc aussi former une suite exacte

$$g_n V/g_n U \longrightarrow g_{n+1} V/g_{n+1} U \longrightarrow 0$$

qui montre que les indices  $(g_n V : g_n U)$  forment une suite décroissante ;

donc stationnaire. Remarquons enfin que tout  $\Lambda$ -module fini est aussi un  $\mathbb{Z}_p$ -module fini. Son ordre est une puissance de  $p$ .

**Proposition 3.3 :** Soit  $V$  un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. Soit  $U = XV + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s$ . Soit  $\alpha$  un quasi-isomorphisme de  $V$  dans  $W$ . Si  $Z = XW + \mathbb{Z}_p \alpha(\tau_1) + \mathbb{Z}_p \alpha(\tau_s)$ , alors il existe un entier  $n_0$  et une constante entière  $c$  tels que pour  $n \geq n_0$ , on ait  $(V : g_n U) = (W : g_n Z) p^c$ .

**Démonstration :** A partir de  $\alpha$  on forme la suite exacte

$$V/g_n U \xrightarrow{\alpha_n} \alpha(V)/\alpha(g_n U) \longrightarrow 0.$$

Le noyau de  $\alpha_n$  est  $(\text{Ker } \alpha + g_n U)/g_n U \cong \text{Ker } \alpha / (\text{Ker } \alpha \cap g_n U)$ . Cet ensemble est fini : De plus  $g_{n+1} U \subset g_n U$ . Donc  $(\text{Ker } \alpha : \text{Ker } \alpha \cap g_n U)$  est une suite croissante et bornée. Donc stationnaire. Donc  $|\text{Ker } \alpha_n|$  est constant pour  $n$  assez grand. Il s'en suit que  $(V : g_n U) / (\alpha(V) : \alpha(g_n U))$  est fini et constant pour  $n$  assez grand. D'autre part,  $(W : \alpha(V))$  est fini. Comme  $V/U$  est fini,  $\alpha(V)/\alpha(U)$  est fini. Donc  $(W : \alpha(U))$  est fini et  $Z/\alpha(U)$  est fini. L'application du lemme 3.2 montre que à partir d'un certain rang  $(g_n Z : g_n \alpha(U))$  est constant. D'où le résultat.

Etudions maintenant les  $\Lambda$ -modules élémentaires, c'est-à-dire les  $\Lambda$ -modules qui apparaissent dans le théorème 2.9 :

**Proposition 3.4 :** Considérons  $\Lambda$  comme  $\Lambda$ -module. Pour toute suite  $(\tau_1, \dots, \tau_s)$  de  $\Lambda^S$ ,  $\Lambda$  n'est pas un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa.

**Démonstration :** Soit  $(\tau_1, \dots, \tau_s)$  dans  $\Lambda^S$ . Nous avons

$g_n (X\Lambda + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s) \subset g_n \Lambda$  et une suite exacte

$$\Lambda/g_n (X\Lambda + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s) \longrightarrow \Lambda/g_n \Lambda \longrightarrow 0.$$

Mais  $g_n$  est distingué. Donc  $\Lambda/g_n \Lambda \cong \mathbb{Z}_p[X]/g_n \mathbb{Z}_p[X]$  est un  $\mathbb{Z}_p$ -module libre de dimension  $d^0 g_n = p^n - 1$ . Donc il est infini.

**Proposition 3.5 :** Soit  $m$  un entier positif. Soit  $V = \Lambda/p^m \Lambda$ . Pour tout  $\tau_1, \dots, \tau_s$  appartenant à  $V$ ,  $V$  est un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. Il existe un entier  $n_0$  et une constante entière  $c$  tels que pour  $n \geq n_0$ , on ait  $|V/g_n(XV + \sum_p \tau_1 + \dots + \sum_p \tau_s)| = p^{mp^n + c}$ .

**Démonstration :** Posons  $U = XV + \sum_p \tau_1 + \dots + \sum_p \tau_s$ . L'indice  $(g_n V : g_n U)$  est constant à partir d'un certain rang d'après le lemme 3.2. D'autre part, on a :  $V/g_n V = (\Lambda/p^m V)/g_n (\Lambda/p^m V) \cong (\Lambda/p^m \Lambda)/(p^m \Lambda + g_n \Lambda)/p^m \Lambda \cong \Lambda/(p^m \Lambda + g_n \Lambda) \cong (\Lambda/g_n \Lambda)/(p^m \Lambda + g_n \Lambda)/g_n \Lambda \cong (\Lambda/g_n \Lambda)/p^m (\Lambda/g_n \Lambda)$ . Mais  $g_n$  est distingué. Donc  $\Lambda/g_n \Lambda \cong \mathbb{Z}_p[X]/g_n \mathbb{Z}_p[X]$ . Donc  $V/g_n V \cong (\mathbb{Z}_p[X]/g_n \mathbb{Z}_p[X])/p^m (\mathbb{Z}_p[X]/g_n \mathbb{Z}_p[X])$ . Mais  $d^0 g_n = p^n - 1$ . Donc  $|V/g_n V| = p^{m(p^n - 1)}$ . D'où le résultat.

**Proposition 3.6 :** Soit  $f$  un polynôme de  $\mathbb{Z}_p[X]$  distingué, de degré  $d$ . Soit  $V = \Lambda/f \Lambda$ . On suppose que  $(\tau_1, \dots, \tau_s)$  sont des éléments de  $V$  tels que  $V$  soit un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. Alors il existe un entier  $n_0$  et une constante entière  $c$  tels que pour  $n \geq n_0$ , on ait :

$$|V/g_n(XV + \sum_p \tau_1 + \dots + \sum_p \tau_s)| = p^{dn + c}$$

La démonstration de cette proposition utilise le lemme :

**Lemme :** Pour  $n$  assez grand, il existe des polynômes  $A_n$  et  $B_n$  tels que  $g_{n+1} = g_n(p(1 + A_n p) + B_n f)$ .

**Démonstration du lemme :** On a dans  $\Lambda$  la congruence  $f \equiv X^d \pmod{p}$ . Si  $n_1$  est tel que  $p^{n_1} \geq d$ , alors  $X^{p^{n_1}} \equiv 0 \pmod{(f, p)}$ . Donc  $X^{p^n} \equiv 0 \pmod{(f, p)}$  pour  $n \geq n_1$ . Mais  $(1 + X)^{p^n} \equiv 1 + X^{p^n} \pmod{p}$ . Donc  $(1 + X)^{p^n} \equiv 1 \pmod{(f, p)}$

et un calcul évident montre que  $(1 + X)^{p^{n+1}} \equiv 1 \pmod{(f, p^2)}$ . On en déduit  $1 + (1 + X)^{p^{n+1}} + \dots + (1 + X)^{(p-1)p^{n+1}} \equiv p \pmod{(f, p^2)}$ .

C'est-à-dire il existe  $A_{n+1}$  et  $B_{n+1}$  tels que

$$1 + (1 + X)^{p^{n+1}} + \dots + (1 + X)^{(p-1)p^{n+1}} = p + A_{n+1} p^2 + B_{n+1} f.$$

Démonstration de la proposition : Considérons le quotient  $g_n V / g_{n+1} V$ .

Pour  $n$  assez grand, nous déduisons du lemme l'égalité :  $g_{n+1} V = g_n p V$  ; car  $f$  annule  $V$  et  $1 + A_n p$  est un élément inversible de  $\Lambda$ .

D'autre part, si  $U = X V + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s$ , nous avons  $U \subset V$  et  $g_n U \subset g_n V \subset V$ . L'hypothèse  $(V : g_n U)$  fini implique donc  $(V : g_n V)$  est fini. Comme  $f$  est distingué,  $V$  est isomorphe à  $\mathbb{Z}_p[X]/f\mathbb{Z}_p[X]$  et  $V$  est un  $\mathbb{Z}_p$ -module libre de dimension  $d$ . Il en est de même de  $g_n V$ , pour tout  $n$ .

De l'égalité  $g_{n+1} V = g_n p V$ , pour  $n$  assez grand, on déduit que

$(g_n V : g_{n+1} V) = p^d$ . Il existe donc une constante  $c_0$ , telle que pour  $n$  assez grand  $(V : g_n V) = p^{dn + c_0}$ . Il reste à s'occuper de l'indice  $(g_n V : g_n U)$ .

Le lemme 3.2 permet de conclure qu'il est constant pour  $n$  assez grand. D'où le résultat.

Remarque : On désigne toujours par  $f$  un polynôme distingué. Lorsqu'il existe un entier  $n$  tel que  $f$  et  $g_n$  ne soient pas premiers entre eux, alors pour tout  $\tau_1, \dots, \tau_s$  appartenant à  $\Lambda/f\Lambda$ ,  $\Lambda/f\Lambda$  n'est pas un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. Par contre, si  $f$  est premier à  $h_n$  pour tout  $n$ , alors pour tout  $\tau_1, \dots, \tau_s$  appartenant à  $\Lambda/f\Lambda$ ,  $\Lambda/f\Lambda$  est un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. Quant au module  $\Lambda/X^d\Lambda$ , il peut, suivant les valeurs de  $\tau_1, \dots, \tau_s$ , être ou ne pas être un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa.

Proposition 3.7 : Soit  $V$  un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. On suppose que  $V$  se décompose en somme directe de deux modules  $V = V' \oplus V''$ . Posons  $\tau_i = \tau_i' + \tau_i''$  avec  $\tau_i' \in V'$  et  $\tau_i'' \in V''$ . Alors  $V'$  est un  $(\tau_1', \dots, \tau_s')$ -

module d'Iwasawa et  $V''$  est un  $(\tau_1'', \dots, \tau_s'')$ -module d'Iwasawa.

Soit  $U = X V + \sum_p \tau_1 + \dots + \sum_p \tau_s$  ; soit  $U' = X V' + \sum_p \tau_1' + \dots + \sum_p \tau_s'$  et  $U'' = X V'' + \sum_p \tau_1'' + \dots + \sum_p \tau_s''$ . Il existe un entier  $n_0$  et une constante  $c$  tels que  $n \geq n_0$  implique :

$$(V : g_n U) = (V' : g_n U') (V'' : g_n U'') p^c.$$

**Démonstration** : La première affirmation se déduit de la proposition 3.1. Ensuite nous avons  $\sum_p \tau_1 \subset \sum_p \tau_1' + \sum_p \tau_1''$ , d'où  $U \subset U' \oplus U''$  ; soit encore  $g_n U \subset g_n U' \oplus g_n U''$ . D'autre part,  $V/g_n(U' \oplus U'')$  est isomorphe à  $V'/g_n U' \oplus V''/g_n U''$ . Pour conclure, on applique le lemme 3.2 à  $U' \oplus U''$  et  $U$  : Il existe un entier  $n_0$  et une constante  $c$  tels que : pour  $n \geq n_0$ , on ait :  $(g_n(U' \oplus U'') : g_n U) = p^c$ .

**Théorème 3.8** : Soit  $V$  un  $\Lambda$ -module. Si  $\tau_1, \dots, \tau_s$  sont des éléments de  $V$  et si  $V$  est un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa, alors il existe des entiers positifs  $n_0, \mu, \lambda$  et un entier relatif  $\nu$  tels que  $n \geq n_0$  implique :

$$|V/g_n(XV + \sum_p \tau_1 + \dots + \sum_p \tau_s)| = p^\mu p^{n+\lambda n+\nu}.$$

**Démonstration** : Par définition,  $V$  est un  $\Lambda$ -module de type fini. Utilisons le théorème 2.9 : il existe un entier  $r$ , des polynômes distingués  $f_1, \dots, f_t$ , des entiers  $m_1, \dots, m_u$  et un quasi-isomorphisme de  $V$  dans  $\Lambda^r \oplus \left( \bigoplus_i (\Lambda/f_i \Lambda) \right) \oplus \left( \bigoplus_i (\Lambda/p^{m_i} \Lambda) \right)$ . D'après la proposition 3.1, ce  $\Lambda$ -module est un module d'Iwasawa. Donc chaque composante aussi (proposition 3.7). On déduit alors de la proposition 3.4 que  $r = 0$ . L'application des propositions 3.3, 3.5, 3.6 et 3.7 fait apparaître les entiers  $\mu = \sum m_i$  et  $\lambda = \sum d^0 f_i$ .

**Définition** : Nous dirons que  $\mu$  et  $\lambda$  sont les paramètres associés au module d'Iwasawa  $V$ .

Remarques : Ces paramètres,  $\lambda$  et  $\mu$ , ne dépendent pas des valeurs  $\tau_1, \dots, \tau_s$  (bien que  $V$  puisse, suivant ces valeurs, être ou ne pas être un module d'Iwasawa). En effet, supposons que  $V$  soit un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa et aussi un  $(\tau'_1, \dots, \tau'_s)$ -module d'Iwasawa. Alors il est clair que  $V$  est encore un  $(\tau_1, \dots, \tau_s, \tau'_1, \dots, \tau'_s)$ -module d'Iwasawa. Posons  $U = X V + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s$ ,  $U' = X V + \mathbb{Z}_p \tau'_1 + \dots + \mathbb{Z}_p \tau'_s$  et  $W = X V + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s + \mathbb{Z}_p \tau'_1 + \dots + \mathbb{Z}_p \tau'_s$ . L'application du lemme 3.2 à  $W$  et  $U$  d'une part et  $W$  et  $U'$  d'autre part, montre que pour  $n$  assez grand les indices  $(g_n V : g_n U)$  et  $(g_n V : g_n U')$  sont constants.

Les paramètres  $\lambda$  et  $\mu$  sont conservés par quasi-isomorphisme (Proposition 3.3).

Par contre, la quantité  $\nu$  dépend de  $\tau_1, \dots, \tau_s$ . De plus, elle peut être négative comme le montre l'exemple suivant : Soit  $V = \Lambda/p\Lambda$ . Choisissons pour  $\tau$  la classe de  $1 + X$  modulo  $p\Lambda$ . Alors  $V$  est  $\tau$ -module d'Iwasawa. On vérifie que l'on a  $\mu = 1$ ,  $\lambda = 0$  et  $\nu = -1$ .

#### 4 - $\mathbb{Z}_p$ -extensions :

Définition d'une  $\mathbb{Z}_p$ -extension : Une extension  $K_\infty/K_0$  est dite une  $\mathbb{Z}_p$ -extension, si elle est galoisienne et si son groupe de Galois est isomorphe à  $\mathbb{Z}_p$ . On note ce groupe de Galois  $\Gamma$ . Pour tout entier  $n$ ,  $\Gamma/\Gamma^{p^n}$  (on note  $\Gamma$  multiplicativement) est cyclique d'ordre  $p^n$ . Soit  $K_n$  le sous-corps de  $K_\infty$ , contenant  $K_0$  et correspondant par la théorie de Galois à  $\Gamma^{p^n}$ . L'extension  $K_n/K_0$  est cyclique de degré  $p^n$ . Les corps  $K_0, K_1, \dots, K_n, \dots$  forment une suite croissante. Ce sont les seuls sous-corps de  $K_\infty$ . On a évidemment  $K_\infty = \bigcup_{i \geq 0} K_i$ . Remarquons aussi que, pour tout entier  $d$ ,  $K_\infty/K_d$  est aussi une  $\mathbb{Z}_p$ -extension.

La proposition suivante précise la ramification à l'intérieur d'une  $\mathbb{Z}_p$ -extension. Elle résulte de la théorie classique de la ramification :

Proposition 4.1 : Soit  $K_\infty/K_0$  une  $\mathbb{Z}_p$ -extension. Aucun idéal de  $K_0$  premier à  $p$  ne se ramifie dans  $K_\infty/K_0$ . Il existe au moins un idéal de  $K_0$  au-dessus de  $p$  ramifié dans  $K_\infty/K_0$ . Si  $\mathfrak{p}$  est un tel idéal, il existe un entier  $n_p$  tel que  $K_\infty/K_{n_p}$  soit totalement ramifiée pour les idéaux au-dessus de  $\mathfrak{p}$  et  $K_{n_p}/K_0$  soit non ramifiée en  $\mathfrak{p}$ . Il existe donc un entier  $d (= \sup_p n_p)$  tel que tout idéal de  $K_d$  soit : ou totalement ramifié dans  $K_\infty/K_d$  ; ou non ramifié dans  $K_\infty/K_d$ .

Introduisons maintenant l'algèbre  $\Lambda$  : Nous désignons toujours par  $K_\infty/K_0$  une  $\mathbb{Z}_p$ -extension. Soit  $\gamma$  un  $\mathbb{Z}_p$ -générateur de  $\Gamma$  : nous voulons dire par là que si nous choisissons un isomorphisme de  $\mathbb{Z}_p$  sur  $\Gamma$ ,  $\gamma$  est l'image de 1 par cet isomorphisme et  $\gamma^u$  est l'image de  $u$ . Soit  $\Gamma_n = \Gamma/\Gamma^{p^n}$  et soit  $\gamma_n$  la classe de  $\gamma$  modulo  $\Gamma^{p^n}$ , c'est-à-dire la restriction de  $\gamma$  à  $K_n$ . Le groupe  $\Gamma_n$  est cyclique d'ordre  $p^n$  et  $\gamma_n$  en est un générateur.

On considère l'isomorphisme

$$\mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[T]/(T^{p^n} - 1)\mathbb{Z}_p[T],$$

induit par l'application :

$$\begin{cases} \mathbb{Z}_p[T] \rightarrow \mathbb{Z}_p[\Gamma_n] \\ T \rightarrow \gamma_n. \end{cases}$$

Changeons  $T$  en  $X+1$ . On a donc un isomorphisme :

$$\mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[X]/((1+X)^{p^n} - 1)\mathbb{Z}_p[X].$$

induit par l'application

$$\begin{cases} \mathbb{Z}_p[X] \rightarrow \mathbb{Z}_p[\Gamma_n] \\ 1+X \rightarrow \gamma_n. \end{cases}$$

Comme le polynôme  $h_n = (1+X)^{p^n} - 1$  est distingué, nous avons un isomorphisme (Proposition 1.2) :

$$\mathbb{Z}_p[X]/h_n \mathbb{Z}_p[X] \cong \Lambda/h_n \Lambda,$$

induit par l'injection canonique :  $\mathbb{Z}_p[X] \rightarrow \Lambda$ .

Considérons maintenant le système projectif formé par les  $\mathbb{Z}_p[\Gamma_n]$ .  
 Les homomorphismes utilisés :  $\mathbb{Z}_p[\Gamma_{n+1}] \rightarrow \mathbb{Z}_p[\Gamma_n]$  sont induits par les

$$\text{restrictions : } \begin{cases} \Gamma_{n+1} \rightarrow \Gamma_n \\ \gamma_{n+1} \rightarrow \gamma_n. \end{cases}$$

D'autre part,  $h_n$  divise  $h_{n+1}$  et nous pouvons considérer le système projectif formé des  $\Lambda/h_n\Lambda$ , avec les homomorphismes naturels :

$\Lambda/h_{n+1}\Lambda \rightarrow \Lambda/h_n\Lambda$ . Avec les isomorphismes définis plus haut, nous avons des diagrammes commutatifs :

$$\begin{array}{ccc} \mathbb{Z}_p[\Gamma_{n+1}] & \cong & \Lambda/h_{n+1}\Lambda \\ \downarrow & & \downarrow \\ \mathbb{Z}_p[\Gamma_n] & \cong & \Lambda/h_n\Lambda \end{array}$$

qui montrent l'existence d'un isomorphisme de limites projectives :

$$\lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n] \cong \lim_{\leftarrow} \Lambda/h_n\Lambda.$$

Remarquons, avant d'énoncer la proposition suivante, que  $\lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n]$  contient  $\lim_{\leftarrow} \Gamma_n = \Gamma$ . Ainsi  $\Gamma$  apparaît comme un sous-groupe du groupe multiplicatif de la  $\mathbb{Z}_p$ -algèbre  $\lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n]$ .

**Proposition 4.2 :** Les  $\mathbb{Z}_p$ -algèbres  $\lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n]$  et  $\Lambda = \mathbb{Z}_p[[X]]$  sont isomorphes. Cet isomorphisme fait correspondre  $X + 1$  à  $\gamma$ .

**Démonstration :** Nous allons montrer que  $\lim_{\leftarrow} \Lambda/h_n\Lambda$  et  $\Lambda$  sont isomorphes : on considère les surjections canoniques :  $\Lambda \rightarrow \Lambda/h_n\Lambda$  et on en déduit un  $\mathbb{Z}_p$ -homomorphisme :

$$\Lambda \rightarrow \lim_{\leftarrow} \Lambda/h_n\Lambda$$

qui associe à  $\lambda$  la suite  $(\lambda + h_n\Lambda)_{n \in \mathbb{N}}$ . Montrons qu'il s'agit d'un isomorphisme.

Nous avons  $h_{n+1}/h_n = 1 + (1+X)^{p^n} + \dots + (1+X)^{p^n(p-1)}$  et ce polynôme appartient à l'idéal maximal de  $\Lambda : (p, X)$ . On en déduit que  $h_n$  appar-



tient à  $(p, X)^{n+1}$ . Cet idéal est l'ensemble des séries de la forme  $p^{n+1} a_0 + p^n a_1 X + \dots + p a_n X^n + a_{n+1} X^{n+1} + \dots$ ;  $a_0, a_1, \dots, a_n, \dots$  étant des éléments de  $\mathbb{Z}_p$ . On voit donc que l'intersection  $\bigcap_{n \in \mathbb{N}} (p, X)^n$  est réduite à  $\{0\}$ . Il en est de même de l'intersection  $\bigcap_{n \in \mathbb{N}} h_n \Lambda$ . Ceci montre que l'homomorphisme considéré est injectif,

Pour démontrer la surjectivité, le concept suivant de limite semble utile : Si  $(\lambda_n)_{n \in \mathbb{N}}$  est une suite d'éléments de  $\Lambda$ , et si  $\lambda_n = \sum_{i \in \mathbb{N}} a_{ni} X^i$ , on dira que  $\lim_{n \rightarrow \infty} \lambda_n$  existe si  $\lim_{n \rightarrow \infty} a_{ni}$  existe pour tout  $i$ . On pose évidemment  $\lim_{n \rightarrow \infty} \lambda_n = \sum_{i \in \mathbb{N}} \left( \lim_{n \rightarrow \infty} a_{ni} \right) X^i$ .

Le lemme suivant est évident :

Lemme : Soit une suite  $(\mu_i)_{i \in \mathbb{N}}$  d'éléments de  $\Lambda$ , telle que pour tout  $i$ ,  $\mu_i$  appartienne à  $(p, X)^i$ . Soit  $\lambda_n = \sum_{i=0}^n \mu_i$ . Alors la suite  $(\lambda_n)_{n \in \mathbb{N}}$  converge au sens défini plus haut.

Revenons maintenant à l'homomorphisme considéré : Soit  $(\lambda_n + h_n \Lambda)_{n \in \mathbb{N}}$  un élément de  $\varprojlim \Lambda/h_n \Lambda$ . Posons  $\lambda_{n+1} = \lambda_n + h_n \mu_n$ . Nous avons donc  $\lambda_n = \lambda_0 + \mu_0 h_0 + \dots + \mu_{n-1} h_{n-1}$ . Comme  $h_i$  appartient à  $(p, X)^{i+1}$ , on déduit du lemme précédent la convergence de la suite  $(\lambda_n)_{n \in \mathbb{N}}$  : Soit  $\lambda = \lim_{n \rightarrow \infty} \lambda_n$ . Lorsque  $m > n$ , nous avons aussi :

$$\lambda_m - \lambda_n = h_n [\mu_m h_m / h_n + \mu_{m-1} h_{m-1} / h_n + \dots + \mu_n].$$

Désignons par  $v_{m,n}$  la quantité entre crochets. Utilisant à nouveau le lemme, nous voyons que la suite  $(v_{m,n})_{m \in \mathbb{N}}$  converge. Soit  $v_n$  sa limite. Nous avons alors  $\lambda - \lambda_n = h_n v_n$  et ceci montre que  $\lambda + h_n \Lambda = \lambda_n + h_n \Lambda$ . Ainsi,  $\lambda$  est l'antécédent de  $(\lambda_n + h_n \Lambda)_{n \in \mathbb{N}}$ . Nous avons montré que l'homomorphisme considéré, de  $\Lambda$  dans  $\varprojlim \Lambda/h_n \Lambda$ , est un isomorphisme. Dans cet isomorphisme  $1 + X$  correspond à  $(1 + X + h_n \Lambda)_{n \in \mathbb{N}}$ . Dans  $\varprojlim \mathbb{Z}_p[\Gamma_n]$ ,  $1 + X$

correspond donc à la suite  $(\gamma_n)_{n \in \mathbb{N}}$  et cette suite n'est autre que  $\gamma$ , puisque l'on a identifié  $\varprojlim \Gamma_n$  et  $\Gamma$ .

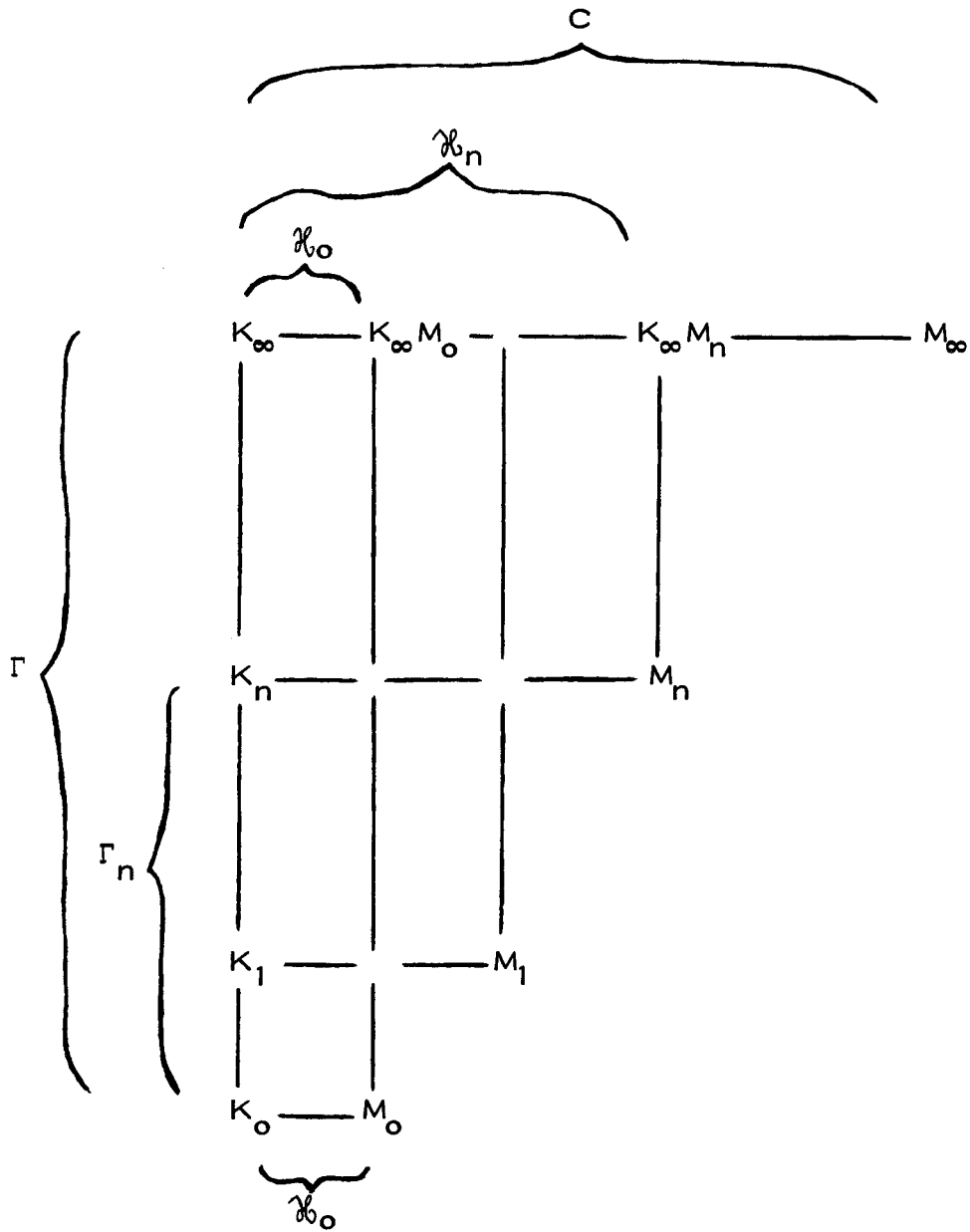
Définition de  $\mathcal{H}_i$  et du  $\Lambda$ -module  $C$  : On conserve les mêmes notations. Soit  $\mathcal{H}_i$  le  $p$ -groupe des classes d'idéaux de  $K_i$ . La suite  $(\mathcal{H}_i)_{i \in \mathbb{N}}$  constitue, avec les applications normes un système projectif, dont on nomme la limite  $C$ .

$$C = \varprojlim \mathcal{H}_i.$$

Comme chaque  $\mathcal{H}_i$  est un  $\mathbb{Z}_p[\Gamma_i]$ -module,  $C$  se trouve donc être un module sur  $\varprojlim \mathbb{Z}_p[\Gamma_i]$ . En vertu de l'isomorphisme de la proposition 4.2,  $C$  est donc un  $\Lambda$ -module.

Définition de  $\tau_1, \tau_2, \dots, \tau_s$  : Nous supposons désormais que tous les idéaux de  $K_0$  sont non ramifiés dans  $K_\infty/K_0$ , sauf  $s$  d'entre eux notés  $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_s$ . Nous les supposerons totalement ramifiés dans  $K_\infty/K_0$ . Cette hypothèse ne restreint pas la généralité du résultat que nous avons en vue : en effet, d'une part, on ne cherche à obtenir que des résultats "asymptotiques" c'est-à-dire valables à partir d'une certaine hauteur dans la  $\mathbb{Z}_p$ -extension et d'autre part, nous avons vu que la ramification d'une  $\mathbb{Z}_p$ -extension est ainsi faite, au moins à partir d'un certain rang (Proposition 4.1).

Soit  $M_i$  le  $p$ -corps de classe de Hilbert de  $K_i$ . Cela veut dire que  $M_i/K_i$  est la  $p$ -extension abélienne non ramifiée maximale de  $K_i$ . Dans l'isomorphisme de réciprocité,  $\text{Gal}(M_i/K_i)$  est isomorphe à  $\mathcal{H}_i$ . L'extension  $M_i/K_0$  est galoisienne et le groupe  $\text{Gal}(K_i/K_0) = \Gamma_i$  opère sur  $\text{Gal}(M_i/K_i)$  par conjugaison. Ainsi  $\text{Gal}(M_i/K_i)$  et  $\mathcal{H}_i$  sont des  $\mathbb{Z}[\Gamma_i]$ -modules isomorphes.



Soit  $M_\infty = \bigcup_{i \in \mathbb{N}} M_i$ . L'extension  $M_\infty/K_0$  est galoisienne et on note  $G$  son groupe de Galois. Nous avons aussi  $M_\infty = \bigcup_{i \in \mathbb{N}} (M_i K_\infty)$  et  $\text{Gal}(M_i K_\infty/K_\infty) \cong \text{Gal}(M_i/K_i) \cong \mathcal{H}_i$ . Ainsi  $\text{Gal}(M_\infty/K_\infty) = \varprojlim \text{Gal}(M_i K_\infty/K_\infty)$  est isomorphe à  $\varprojlim \mathcal{H}_i = C$  (la restriction des automorphismes correspond, par le corps de classes, à la norme). Par la suite, nous poserons  $C = \varprojlim (M_\infty/K_\infty)$ . On a évidemment  $G/C \cong \Gamma$  et  $\Gamma$  opère sur  $C$  par conjugaison.

Introduisons maintenant  $I_i$  groupe d'inertie dans  $M_\infty/K_0$  de  $\mathfrak{P}_i$ . Comme  $\mathfrak{P}_i$  est totalement ramifié dans  $K_\infty/K_0$ ,  $G$  est produit semi-direct de  $C$  et  $I_i$ . Par restriction à  $K_\infty$ ,  $I_i$  est isomorphe à  $\Gamma$  et nous désignons par  $\gamma_i$  l'élément de  $I_i$  qui correspond ainsi à  $\gamma$ . Pour  $i$  de 1 à  $s$ , on définit  $\tau_i$  par l'égalité  $\tau_i \gamma_i = \gamma_i$ . Ainsi  $\tau_1 = 1$  et  $\tau_1, \dots, \tau_s$  sont des éléments de  $C$ .

Proposition 4.3 : On suppose que les idéaux ramifiés dans  $K_\infty/K_0$  le sont totalement. Le groupe  $C$  est noté multiplicativement et l'action de  $\varprojlim \mathbb{Z}_p[\Gamma_i]$  sur  $C$  exponentiellement. Pour tout entier  $n$ , on a un isomorphisme :

$$\mathcal{H}_n \cong C / [C^{\gamma-1} \tau_1^{\mathbb{Z}_p} \dots \tau_s^{\mathbb{Z}_p}]^{1+\gamma+\dots+\gamma^{p^n-1}}.$$

Démonstration : Commençons par démontrer l'isomorphisme relatif à  $\mathcal{H}_0$ .

Montrons tout d'abord que  $G'$ , groupe dérivé de  $G$  est égal à  $C^{\gamma-1}$ . L'inclusion  $G' \supset C^{\gamma-1}$  est évidente : en effet si  $c$  appartient à  $C$  et si  $\overset{\circ}{\gamma}$  est un élément de  $G$  prolongeant  $\gamma$ , on a  $c^{\gamma-1} = \overset{\circ}{\gamma}^{-1} c \overset{\circ}{\gamma} c^{-1}$ . Donc  $c^{\gamma-1}$  appartient à  $G'$ . Réciproquement, vérifions que  $G/C^{\gamma-1}$  est abélien : On peut d'abord vérifier que  $C^{\gamma-1}$  est un sous-groupe distingué de  $G$ . Il s'en suit que  $C/C^{\gamma-1}$  est un sous-groupe distingué de  $G/C^{\gamma-1}$ . Le quotient de ces groupes est  $G/C \cong \Gamma$ . Soit  $\overset{\circ}{\gamma}$  un relèvement de  $\gamma$  dans  $G/C^{\gamma-1}$ . Si  $u$  et  $v$  sont deux éléments de  $G/C^{\gamma-1}$ , alors on peut les écrire :  $u = \overset{\circ}{\gamma}^x u'$  et  $v = \overset{\circ}{\gamma}^y v'$  avec  $x, y$  dans  $\mathbb{Z}_p$  et  $u'$  et  $v'$  dans  $C/C^{\gamma-1}$ . Mais  $\Gamma$  opère trivia-

lement sur  $C/C^{Y-1}$ . Cela veut dire  $\overset{\circ}{\gamma}^x u' \overset{\circ}{\gamma}^{-x} = u'$  etc... et  $\overset{\circ}{\gamma}^x, \overset{\circ}{\gamma}^y, u', v'$  permutent entre eux. Donc  $uv = vu$ .

Comme  $M_0$  est l'extension abélienne maximale non ramifiée de  $K_0$ , nous avons  $\text{Gal}(M_\infty/M_0) = G' I_1 I_2 \dots I_s = C^{Y-1} I_1 I_2 \dots I_s$ ; étant entendu que  $I_1 I_2 \dots I_s$  désigne le sous-groupe de  $G$  engendré par  $I_1, I_2$  et  $I_s$ . Nous avons donc  $\text{Gal}(M_\infty/M_0 K_\infty) = [C^{Y-1} I_1 I_2 \dots I_s] \cap C$ . Calculons cette intersection et montrons qu'elle est égale à  $C^{Y-1} \tau_1^{\mathbb{Z}_p} \dots \tau_s^{\mathbb{Z}_p}$ .

Un élément de  $C^{Y-1} I_1 I_2 \dots I_s$  est de la forme :

$c^{Y-1} \gamma_1^{u_1} \gamma_2^{u_2} \dots \gamma_s^{u_s} \gamma_1^{u'_1} \gamma_2^{u'_2} \dots \gamma_s^{u'_s} \dots$  avec  $u_i, u'_i \dots$  dans  $\mathbb{Z}_p$  et  $c$  dans  $C$ . Ceci s'écrit encore :

$c^{Y-1} \gamma_1^{u_1} (\tau_2 \gamma_1)^{u_2} \dots (\tau_s \gamma_1)^{u_s} \gamma_1^{u'_1} (\tau_2 \gamma_1)^{u'_2} \dots (\tau_s \gamma_1)^{u'_s} \dots$

Mais  $G/C^{Y-1}$  est commutatif. Donc  $(\tau_2 \gamma_1)^u C^{Y-1} = \tau_2^u \gamma_1^u C^{Y-1}$  pour tout  $u$  de  $\mathbb{Z}$ . En passant à la limite (car  $G/C^{Y-1}$  est un  $\mathbb{Z}_p$ -module) nous avons

$(\tau_2 \gamma_1)^{u_2} \equiv \tau_2^{u_2} \gamma_1^{u_2} \pmod{C^{Y-1}}$  et l'expression considérée peut s'écrire :

$c^{Y-1} \tau_1^{v_1} \dots \tau_s^{v_s} \gamma_1^w$  avec  $v_1, \dots, v_s$  dans  $\mathbb{Z}_p$ , ainsi que  $w$ . Si cette

expression appartient à  $C$ , alors  $\gamma_1^w = 1$  donc elle appartient à

$C^{Y-1} \tau_1^{\mathbb{Z}_p} \dots \tau_s^{\mathbb{Z}_p}$ . Nous avons démontré l'inclusion :

$$([C^{Y-1} I_1 I_2 \dots I_s] \cap C) \subset (C^{Y-1} \tau_1^{\mathbb{Z}_p} \dots \tau_s^{\mathbb{Z}_p}).$$

L'inclusion réciproque est évidente.

Nous déduisons de ces considérations :

$$\text{Gal}(M_\infty/M_0 K_\infty) = C^{Y-1} \tau_1^{\mathbb{Z}_p} \dots \tau_s^{\mathbb{Z}_p}$$

d'où  $\text{Gal}(M_0 K_\infty/K_\infty) \cong C/C^{Y-1} \tau_1^{\mathbb{Z}_p} \dots \tau_s^{\mathbb{Z}_p}$ . Mais il est clair que :

$$\mathcal{H}_0 \cong \text{Gal}(M_0/K_0) \cong \text{Gal}(M_0 K_\infty/K_\infty). \text{ D'où le résultat pour } \mathcal{H}_0.$$

L'isomorphisme relatif à  $\mathcal{H}_n$  se démontre de la même façon :

si on remplace  $K_0$  par  $K_n$ , il faut remplacer  $\gamma$  par  $\gamma^{p^n}$ ,  $\gamma_i$  par  $\gamma_i^{p^n}$ .

Que devient  $\tau_i$  ? Nous avons  $\gamma_i = \tau_i \gamma_1$ .

$$\begin{aligned} \text{D'où } \gamma_i^{p^n} &= (\tau_i \gamma_1)^{p^n} = \tau_i \gamma_1 \tau_i \gamma_1^{-1} \gamma_1^2 \tau_i \gamma_1^{-2} \gamma_1^3 \dots \gamma_1^{-(p^n-1)} \gamma_1^{p^n} \\ &= \tau_i \tau_i^\gamma \tau_i^{\gamma^2} \dots \tau_i^{\gamma^{p^n-1}}. \text{ D'où } \gamma_i^{p^n} = \tau_i^{1+\gamma+\dots+\gamma^{p^n-1}} \gamma_1^{p^n}. \end{aligned}$$

On en déduit l'isomorphisme annoncé.

Il reste pour terminer à montrer que  $C$  est un  $\Lambda$ -module de type fini. Pour cela, on utilise le lemme de Nakayama :

Lemme de Nakayama : Soit  $R$  un  $\Lambda$ -module compact tel que  $R/(p, X)R = 0$ . Alors  $R = 0$ .

Démonstration : L'anneau  $\Lambda$  est muni de la topologie  $(p, X)$ -adique (la notion de limite déjà employée au cours de la démonstration de la proposition 4.2 coïncide avec cette topologie). Soit  $V$  un voisinage de 0 dans  $R$ . Soit  $r$  un élément de  $R$ . Il existe un entier  $n_r$  et un voisinage  $V_r$  de  $r$  tel que  $(p, X)^{n_r} V_r \subset V$ . Comme  $R = \bigcup_{r \in R} V_r$  il existe  $r_1, \dots, r_m$  dans  $R$  tels que  $R = \bigcup_{i=1}^m V_{r_i}$ . Soit  $n$  le plus grand des  $n_{r_i}$ . On a alors  $(p, X)^n R \subset V$ . Mais l'hypothèse  $R/(p, X)R = 0$  implique  $R = (p, X)R = \dots = (p, X)^n R$ . Donc  $R \subset V$  et  $R = 0$ .

Conséquence : Soit  $M$  un  $\Lambda$ -module compact tel que  $M/(p, X)M$  soit un  $\mathbb{F}_p$ -espace vectoriel de dimension finie. Alors  $M$  est un  $\Lambda$ -module de type fini.

Démonstration : Soit  $m_1, \dots, m_n$  des éléments de  $M$  tels que  $(m_i + (p, X)M)_{1 \leq i \leq n}$  forment une base de  $M/(p, X)M$ . Soit  $p = \Lambda m_1 + \Lambda m_2 + \dots + \Lambda m_n$ . Le quotient  $M/P$  est un  $\Lambda$ -module compact tel que  $(M/P)/(p, X)(M/P) = 0$ . Donc le lemme précédent montre que  $M/P = 0$  et  $m_1, \dots, m_n$  est un système de générateurs de  $M$ .

Proposition 4.4 : On conserve les mêmes hypothèses et les mêmes notations qu'à la proposition précédente. Le  $\Lambda$ -module  $C = \varprojlim \mathcal{H}_i$  est un  $\Lambda$ -module de type fini.

Démonstration : Notons un instant  $C$  additivement. Nous avons vu, dans la proposition précédente, que le quotient  $C / (XC + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s)$  est isomorphe à  $\mathcal{H}_0$ , donc est fini. D'autre part,  $(XC + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s) / XC$  est un  $\mathbb{Z}_p$ -module de type fini. Donc  $C/XC$  est un  $\mathbb{Z}_p$ -module de type fini. Il en est donc de même de  $C / (p, X)C$ . D'autre part,  $C$ , limite projective de groupes finis, est compact. Le lemme de Nakayama permet donc de conclure.

On déduit des propositions 4.3 et 4.4 la proposition :

Proposition 4.5 : On conserve les mêmes hypothèses et les mêmes notations qu'à la proposition précédente. Le  $\Lambda$ -module  $C = \varprojlim \mathcal{H}_i$  est un  $(\tau_1, \tau_2, \dots, \tau_s)$ -module d'Iwasawa.

Nous déduisons alors du théorème 3.8 et des propositions précédentes le théorème d'Iwasawa :

Théorème 4.6 : Soit  $K_\infty/K_0$  une  $\mathbb{Z}_p$ -extension et soit  $\mathcal{H}_i$  le  $p$ -groupe des classes d'idéaux de  $K_i$ . Il existe des entiers  $n_0, \mu, \lambda$  positifs et un entier  $\nu$  tels que : si  $n \geq n_0$ , alors l'ordre de  $\mathcal{H}_n$  est donné par :

$$|\mathcal{H}_n| = p^\mu p^{n + \lambda n + \nu}.$$

Exemple : Soit  $p$  un nombre premier impair. Notons  $\mathbb{Q}_n$  le sous-corps du corps cyclotomique  $\mathbb{Q}(\zeta_{p^{n+1}})$  tel que le degré  $(\mathbb{Q}(\zeta_{p^{n+1}}) : \mathbb{Q}_n)$  soit égal à  $p-1$ . Posons  $\mathbb{Q}_\infty = \bigcup_{i \geq 1} \mathbb{Q}_i$ . La  $\mathbb{Z}_p$ -extension  $\mathbb{Q}_\infty/\mathbb{Q}$  est l'unique  $\mathbb{Z}_p$ -extension de  $\mathbb{Q}$ . Il n'y a, dans cette extension, qu'un idéal totalement ramifié. Donc  $s = 1$  et  $\mathcal{H}_0 = C/C^{p-1}$ . Comme  $\mathbb{Q}$  est principal,  $\mathcal{H}_0 = \{1\}$  et le lemme de

Nakayama montre que  $C$  est réduit à  $\{1\}$ . Les paramètres associés à  $\mathbb{Q}_\infty/\mathbb{Q}$  vérifient donc :  $\lambda = \mu = \nu = 0$ .

Considérons aussi la  $\mathbb{Z}_p$ -extension dont le corps de base est  $K_0 = \mathbb{Q}(\rho)$  et définie par  $K_n = \mathbb{Q}(\rho^{n+1})$  pour tout  $n$ . Le même argument montre que si  $p$  est régulier, c'est-à-dire si  $\mathcal{K}_0 = \{1\}$ , alors les paramètres  $\lambda, \mu, \nu$  sont nuls.

5 - Lien entre  $p^m$ -rangs et paramètres  $\lambda, \mu$ .

Notation : Si  $H$  est un  $\mathbb{Z}_p$ -module, on note  $\dim_m H$  la dimension du  $\mathbb{F}_p$ -espace vectoriel  $p^{m-1}H/p^mH$ . C'est le  $p^m$ -rang de  $H$ .

Proposition 5.1 : Soit  $V$  un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. On pose  $U = XV + \mathbb{Z}_p \tau_1 + \dots + \mathbb{Z}_p \tau_s$ . Soit  $\alpha$  un quasi-isomorphisme de  $V$  dans  $W$ . Nous savons (Proposition 3.1) que  $W$  est un  $(\alpha(\tau_1), \dots, \alpha(\tau_s))$ -module d'Iwasawa. Posons  $T = XW + \mathbb{Z}_p \alpha(\tau_1) + \dots + \mathbb{Z}_p \alpha(\tau_s)$ . Alors la suite

(double)  $\left[ \sum_{i=1}^m [\dim_i (V/g_n U) - \dim_i (W/g_n T)] \right]_{\substack{n \geq 0 \\ m \geq 0}}$  est bornée.

Démonstration : Nous avons  $|V/g_n U + p^m V| = p^{\sum_{i=1}^m \dim_i (V/g_n U)}$  et de même pour  $|W/g_n T + p^m W|$ .

A partir de  $\alpha$ , on forme la suite exacte :

$$0 \longrightarrow \frac{\text{Ker } \alpha}{\text{Ker } \alpha \cap (g_n U + p^m V)} \longrightarrow \frac{V}{g_n U + p^m V} \longrightarrow \frac{\alpha(V)}{g_n \alpha(U) + p^m \alpha(V)} \longrightarrow 0.$$

Le premier terme est fini et son ordre est borné par  $|\text{Ker } \alpha|$ . Ensuite, les deux suites exactes évidentes suivantes :

$$0 \longrightarrow \frac{\alpha(V)}{g_n \alpha(U) + p^m \alpha(V)} \longrightarrow \frac{W}{g_n \alpha(U) + p^m \alpha(V)} \longrightarrow \frac{W}{\alpha(V)} \longrightarrow 0,$$

$$0 \longrightarrow \frac{g_n T + p^m W}{g_n \alpha(U) + p^m \alpha(V)} \longrightarrow \frac{W}{g_n \alpha(U) + p^m \alpha(V)} \longrightarrow \frac{W}{g_n T + p^m W} \longrightarrow 0,$$



conduisent à étudier le quotient  $\frac{g_n T + p^m W}{g_n \alpha(U) + p^m \alpha(V)}$ . Pour cela, on forme

la suite exacte :  $\frac{T}{\alpha(U)} \times \frac{W}{\alpha(V)} \rightarrow \frac{g_n T + p^m W}{g_n \alpha(U) + p^m \alpha(V)} \rightarrow 0$  en associant

aux classes de  $t$  et  $w$  modulo  $\alpha(U)$  et  $\alpha(V)$  la classe de  $g_n t + p^m w$  modulo  $g_n \alpha(U) + p^m \alpha(V)$ . Par hypothèse le groupe  $W/\alpha(V)$  est fini,

L'autre aussi, car on a des suites exactes :

$$\frac{W}{\alpha(V)} \rightarrow \frac{XW}{X\alpha(V)} \rightarrow 0 \quad \text{et} \quad \frac{XW}{X\alpha(V)} \rightarrow \frac{XW + \sum_p \alpha(\tau_1) + \dots + \sum_p \alpha(\tau_s)}{X\alpha(V) + \sum_p \alpha(\tau_1) + \dots + \sum_p \alpha(\tau_s)} \rightarrow 0.$$

Ce dernier quotient est  $T/\alpha(U)$ . Il est donc fini. Ainsi l'ordre de

$$\frac{g_n T + p^m W}{g_n \alpha(U) + p^m \alpha(V)}$$

est borné. D'où le résultat annoncé.

**Proposition 5.2 :** Soit  $V$  un  $(\tau_1, \dots, \tau_s)$ -module d'Iwasawa. On pose encore  $U = XV + \sum_p \tau_1 + \dots + \sum_p \tau_s$ . On suppose que  $V$  est somme directe :  $V = V' \oplus V''$ , de deux sous  $\Lambda$ -modules. Soient  $\tau_i = \tau_i' + \tau_i''$  les décompositions correspondantes et  $U' = XV' + \sum_p \tau_1' + \dots + \sum_p \tau_s'$  et  $U'' = XV'' + \sum_p \tau_1'' + \dots + \sum_p \tau_s''$ . Alors la suite (double)

$$\left[ \sum_{i=1}^m [\dim_i (V/g_n U) - \dim_i (V'/g_n U') - \dim_i (V''/g_n U'')] \right]_{\substack{n \geq 0 \\ m \geq 0}}$$

est bornée.

**Démonstration :** Posons  $T = U' \oplus U''$ . Nous avons

$$V/g_n T = V'/g_n U' \oplus V''/g_n U'' \text{ d'où :}$$

$$\sum_{i=1}^m [\dim_i V'/g_n U' + \dim_i V''/g_n U''] = \sum_{i=1}^m \dim_i V/g_n T$$

et il reste à étudier  $\sum_{i=1}^m [\dim_i V/g_n U - \dim_i V/g_n T]$  ; c'est-à-dire à comparer les deux quotients  $V/g_n U + p^m V$  et  $V/g_n T + p^m V$ . Mais nous avons  $T \supset U$  et une suite exacte évidente :

