

SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Classes des corps cyclotomiques

Séminaire N. Bourbaki, 1960, exp. n° 174, p. 83-93

http://www.numdam.org/item?id=SB_1958-1960__5__83_0

© Association des collaborateurs de Nicolas Bourbaki, 1960, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) 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/>

CLASSES DES CORPS CYCLOTOMIQUES

par Jean-Pierre SERRE

(d'après K. IWASAWA [2], [3], [4], [5])

1. Énoncé des principaux résultats.

Soit p un nombre premier, qui restera fixé dans tout ce qui suit, et soit K_n le corps des racines p^{n+1} -ièmes de l'unité. C'est une extension abélienne de \mathbb{Q} ; le groupe de Galois $G(K_n/\mathbb{Q})$ est isomorphe au groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/p^{n+1}\mathbb{Z}$.

Soit h_n l'ordre du groupe des classes d'idéaux de K_n , et soit p^{e_n} la plus grande puissance de p divisant h_n .

THÉOREME 1 (IWASAWA [2]). - Si $e_1 = 0$ (i.e. si p est un nombre premier "régulier" au sens de Kummer), on a $e_n = 0$ pour tout n .

Pour $p = 2$, on retrouve un résultat de Weber (cf. HASSE [1], paragraphe 34).

THÉOREME 2 (IWASAWA [3]). - Pour chaque nombre premier p , il existe des entiers m, ℓ, c avec $m \geq 0$ et $\ell > 0$ tels que :

$$(*) \quad e_n = mp^n + \ell n + c \quad \text{pour } n \text{ assez grand.}$$

Comme on le verra au n° 4, ces deux théorèmes se déduisent d'un théorème de structure pour un certain groupe à opérateurs. Ce groupe se construit ainsi : soit X_n la p -composante du groupe des classes d'idéaux de K_n ; c'est un p -groupe abélien fini, d'ordre p^{e_n} , sur lequel opère le groupe de Galois $G(K_n/\mathbb{Q})$ et en particulier son sous-groupe $\Gamma_n = G(K_n/K_0)$. En passant à la limite projective sur n au moyen des homomorphismes $X_{n+1} \rightarrow X_n$ définis par la norme, on obtient un p -groupe abélien compact totalement discontinu X , sur lequel opère le groupe $\Gamma = \varprojlim \Gamma_n$, groupe de Galois de L/K_0 , où L est la réunion des K_n . Si $p \neq 2$, le groupe Γ_n est cyclique d'ordre p^n , et Γ est isomorphe au groupe additif \mathbb{Z}_p des entiers p -adiques. Pour $p = 2$, il faut utiliser K_1 à la place de K_0 .

Dans tout ce qui suit, on notera γ un générateur de Γ , et on posera $\omega_n = 1 - \gamma^{p^n}$. La connaissance du groupe à opérateurs X permet de récupérer

X_n , grâce à la formule :

$$(*) \quad X_n = X/\omega_n X .$$

La structure de X sera déterminée grâce au théorème suivant :

THÉOREME 3 (IWASAWA [3]). - Soit A la limite projective des algèbres sur \mathbb{Z} des groupes Γ_n . Le groupe X est un A -module de type fini et de torsion.

De tels modules peuvent se décrire complètement ("modulo" les groupes finis), et c'est ainsi que l'on aboutit à la définition des entiers ℓ et m . On a $m = 0$ si et seulement si X est un \mathbb{Z}_p -module de type fini ; le rang de ce module est alors ℓ , et γ définit une matrice carrée d'ordre ℓ , à coefficients dans \mathbb{Z}_p . On ne sait presque rien sur les valeurs propres de cette matrice, et c'est dommage : sur les corps de fonctions, dans la situation analogue, ces valeurs propres sont certains zéros d'une fonction ζ .

Les démonstrations des trois théorèmes qui précèdent utilisent uniquement la théorie du corps de classes (pour interpréter X_n comme le groupe de Galois de la p -extension abélienne non ramifiée maximale de K_n). Dans [4], IWASAWA utilise la formule analytique donnant h_n pour donner un critère permettant d'affirmer que $m > 0$: il faut et il suffit que les nombres de Bernoulli vérifient certaines congruences en nombre infini. Le calcul explicite a été fait, paraît-il, pour les trois premiers nombres irréguliers, $p = 37, 59$ et 67 . Dans les trois cas, on a trouvé $m = 0$. Comme dit IWASAWA, cela ne suffit pas pour faire une conjecture ...

Signalons que la limite inductive des X_n est isomorphe à la p -composante de $H^1(\Omega, \mathcal{F})$, où Ω est l'ensemble des valuations de L (muni d'une topologie convenable), et \mathcal{F} le faisceau des unités. Pour plus de détails, voir [5].

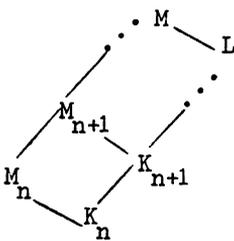
2. Groupes de décomposition et d'inertie.

Soit L/K une extension galoisienne, finie ou infinie, de groupe de Galois $G(L/K)$; soit v une valuation de K , et soit w un prolongement de v à L ; on sait que tout autre prolongement de v est transformé de w par une opération de $G(L/K)$. Soit A_w l'anneau de w , et soit \bar{L}_w son corps des restes. Le groupe de décomposition $D_w(L/K)$ de w est l'ensemble des $\sigma \in G(L/K)$ tels que $\sigma(A_w) = A_w$; le groupe d'inertie $T_w(L/K)$ est l'ensemble des $\sigma \in D_w(L/K)$ qui opèrent trivialement sur \bar{L}_w . Ces groupes sont fermés dans $G(L/K)$, topologisé à la manière habituelle ; ils jouissent de propriétés fonctorielles simples

(passage au sous-groupe et au groupe quotient notamment). On dit que v est non ramifiée dans L si $T_w(L/K) = 0$, cette propriété ne dépendant pas de l'extension w choisie.

On appliquera ce qui précède à des corps de nombres algébriques (non nécessairement finis sur \mathbb{Q}). Les seules valuations de ces corps sont celles qui prolongent les valuations p -adiques de \mathbb{Q} . Si K est un corps de nombres, et L/K une extension galoisienne de K , on dit que L/K est non ramifiée si toutes les valuations de K sont non ramifiées dans L . La notion d'extension non ramifiée est de caractère fini. Plus précisément :

LEMME 1. - Soit L la réunion d'une suite croissante de corps K_n finis sur \mathbb{Q} et soit M/L une extension finie, galoisienne, non ramifiée. Pour n assez grand, il existe alors une extension finie, galoisienne, non ramifiée M_n/K_n telle que $M = M_n \otimes_{K_n} L$.



On construit facilement des extensions galoisiennes M_n/K_n avec $M_n \otimes_{K_n} L = M$ (pour n assez grand). Tout revient à voir que $M_n \cdot K_{n+i}$ est extension non ramifiée de K_{n+i} pour i assez grand, ce qui est un simple exercice de limites projectives (il faut se servir du fait qu'il n'y a qu'un nombre fini de valuations de K_n qui se ramifient dans M_n). Pour plus de détails, voir [3], théorème 6.1.

3. Γ -extensions.

Soit Γ un groupe topologique isomorphe au groupe \mathbb{Z}_{mp} des entiers p -adiques ; comme au n° 1, nous désignons par γ un générateur de Γ .

Une extension algébrique L/K est dite une Γ -extension si elle est galoisienne et si son groupe de Galois est Γ . Il revient au même de dire que L est réunion d'une suite croissante de corps K_n , chaque K_n étant une extension cyclique de K de degré p^n ; les K_n correspondent par la théorie de Galois aux sous-groupes $H_n = p^n \Gamma$ de Γ , et l'on sait que ce sont les seuls sous-groupes fermés de Γ (avec 0).

LEMME 2. - Soit L/K une Γ -extension, et supposons K fini sur \mathbb{Q} . Il existe alors au moins une valuation de K qui se ramifie dans L , et une telle valuation induit sur \mathbb{Q} la valuation p -adique.

D'après la théorie du corps de classes, toute extension abélienne non ramifiée de K est finie ; comme L/K est une extension infinie, il existe au moins une valuation v de K qui se ramifie dans L . Soit T le groupe d'inertie correspondant ; c'est un sous-groupe fermé $\neq 0$ de Γ , donc c'est un groupe isomorphe à \mathbb{Z}_p . D'après la théorie de la ramification supérieure, T est produit d'un groupe fini par un ℓ -groupe, où ℓ est la caractéristique de \overline{K}_v . On a donc nécessairement $\ell = p$, ce qui signifie bien que v induit sur \mathbb{Q} la valuation p -adique.

EXEMPLE. - Le corps L défini au n° 1 est une Γ -extension de K_0 (on suppose $p \neq 2$) ; la seule valuation de K_0 qui soit ramifiée est l'unique valuation v prolongeant la valuation p -adique de \mathbb{Q} . Cette valuation est d'ailleurs totale-ment ramifiée, i.e. on a $T = \Gamma$.

4. Structure de la p -extension abélienne non ramifiée maximale d'une Γ -extension. Cas totalement ramifié.

Si K est un corps de nombres algébriques nous noterons $A_p(K)$ la p -extension abélienne non ramifiée maximale de K , c'est-à-dire la composée des extensions finies M/K , où M/K est une extension abélienne non ramifiée dont le groupe de Galois est un p -groupe.

Soit L/K une Γ -extension, avec K fini sur \mathbb{Q} , et soit $M = A_p(L)$. Nous

X $\left\{ \begin{array}{l} M \\ | \\ L \end{array} \right.$ noterons X le groupe de Galois $G(M/L)$; c'est une limite projective de p -groupes abéliens finis. L'extension M/K est galoisienne résoluble ; le groupe $\Gamma = G(L/K)$ opère sur $X = G(M/L)$ par automorphismes intérieurs.

Γ $\left\{ \begin{array}{l} | \\ K \end{array} \right.$ D'après le lemme 1, le corps M est réunion des corps $M_n = A_p(K_n)$; le groupe X est donc limite projective des groupes $X_n = G(M_n/K_n)$.

D'après la théorie du corps de classes, X_n est isomorphe à la p -composante du groupe des classes d'idéaux du corps K_n ; nos notations sont donc cohérentes avec celles du n° 1. Le groupe X_n est un p -groupe abélien fini, sur lequel opère le groupe $\Gamma_n = G(K_n/K) = \Gamma/p^n \Gamma$; on peut donc munir canoniquement X_n d'une structure de module sur l'anneau $A_n = \mathbb{Z}_p[\Gamma_n]$, algèbre du groupe Γ_n à coefficients dans les entiers p -adiques. Par passage à la limite projective, on munit X d'une structure de module topologique sur l'anneau A limite projective des anneaux A_n ; on verra d'ailleurs au n° 6 que A est isomorphe à l'anneau de séries formelles $\mathbb{Z}_p[[T]]$, l'isomorphisme faisant correspondre au générateur γ de Γ la série formelle $1 - T$.

On se propose maintenant de reconstruire X_n à partir du A -module X (et de certains éléments privilégiés de X) :

Soient v_1, \dots, v_k les valuations de K qui se ramifient dans L (cf. lemme 2), et soient $T_i \subset \Gamma$ les groupes d'inertie correspondants. On a $T_i = p^{n_i} \Gamma$, avec $n_i \geq 0$. Nous supposons dans ce numéro que $n_i = 0$ pour tout i , autrement dit que les valuations v_i sont totalelement ramifiées ; le cas général se ramène facilement à celui-là, cf. n° 5.

Pour tout i , soit w_i un prolongement de v_i à M , et soit $S_i \subset G(M/K)$ le groupe d'inertie correspondant ; puisque M/L est non ramifié, on a $S_i \cap X = 0$; puisque v_i est totalement ramifié dans L , l'image de S_i dans Γ est Γ tout entier. Donc chacun des S_i est un supplémentaire de X dans $G(M/K)$, et $G(M/K)$ est produit semi-direct de S_1 par X . Si $\sigma_i \in S_i$ se projette en γ , on peut écrire $\sigma_i = a_i \sigma_1$, avec $a_i \in X$.

THEOREME 4. - Avec les hypothèses et notations précédentes, on a $X_n = X/Y_n$, où Y_n est le sous- Z_{amp} -module de X défini de la façon suivante :

- i. Y_0 est engendré par les a_i et par $(1 - \gamma)X$.
- ii. $Y_n = \nu_n Y_0$, avec $\nu_n = 1 + \gamma + \gamma^2 + \dots + \gamma^{p^n - 1}$.

DÉMONSTRATION de (i). - Le corps M_0 est évidemment la plus grande extension abélienne non ramifiée de $K_0 = K$ contenue dans M . Son groupe de Galois X_0 est donc égal à $G(M/K)/Z_0$, où Z_0 est le plus petit sous-groupe de $G(M/K)$ contenant le sous-groupe des commutateurs $G(M/K)'$ ainsi que les S_i . La décomposition de $G(M/K)$ en produit semi-direct de S_1 par X montre que $G(M/K)' = (1 - \gamma)X$, d'où aussitôt le résultat.

DÉMONSTRATION de (ii). - Comme L est une Γ -extension de K_n , le résultat ci-dessus s'applique à X_n , à condition de remplacer γ par γ^{p^n} et les σ_i par les $\sigma_i^{p^n}$. Cela a pour effet de remplacer les a_i par les $\nu_n a_i$, car, pour tout entier k , on a :

$$(\sigma_i)^k = (a_i \sigma_1)^k = a_i \cdot \sigma_1^{-1} a_i \sigma_1^{-1} \cdot \sigma_1^{-2} a_i \sigma_1^{-2} \dots \sigma_1^{-k+1} a_i \sigma_1^{-k+1} \cdot \sigma_1^k$$

et en particulier, pour $k = p^n$, cela donne :

$$(\sigma_i)^{p^n} = a_i^{p^n} \cdot (\sigma_1)^{p^n} .$$

On a donc $Y_n = (1 - \gamma^{p^n})X + \nu_n H$, où H est engendré par les a_i . Comme $\nu_n(1 - \gamma) = (1 - \gamma^{p^n})$, ceci s'écrit aussi $Y_n = \nu_n Y_0$, ce qui achève la démonstration.

EXEMPLE. - Lorsque $k = 1$, c'est-à-dire lorsqu'une seule valuation de K se ramifie dans L , on a $a_i = 0$, et le théorème 4 montre que $X_n = X/\omega_n X$; c'est la formule $(**)$ du n° 1. Si en outre $X_0 = 0$, on a $X = \omega_0 X$, et comme ω_0 est dans l'idéal maximal \mathfrak{m} de A , ceci entraîne $X = 0$ (lemme de Nakayama, cf. n° 6), d'où $X_n = 0$ pour tout n , ce qui démontre le théorème 1.

THÉOREME 5. - Le A -module X est un module de torsion de type fini.

On sait que X_n est un groupe fini; le théorème 4 montre donc que $X/\omega_n X$ est un \mathbb{Z} -module de type fini, et de rang $\leq k - 1$ (donc indépendant de n). Le théorème en résulte (cf. n° 6, lemmes 4 et 7).

Le résultat ci-dessus permet d'appliquer les théorèmes de structure du n° 6; si \mathcal{C} désigne la catégorie des groupes finis, on en conclut que X est \mathcal{C} -isomorphe à la somme directe d'un \mathbb{Z} -module libre de rang fini ℓ stable par γ , et de modules isomorphes à $\mathbb{Z}/p^{m_i} \mathbb{Z}$. On pose $m = \sum m_i$.

THÉOREME 6. - Si p^{e_n} est l'ordre de X_n , on a $e_n = mp^n + \ell n + c$ pour n grand, c étant une constante.

Si Y est un p -groupe abélien fini, nous noterons $p^{e(Y)}$ son ordre; $e(Y)$ peut aussi être considéré comme la longueur du A -module Y . D'après le théorème 4, on a $e_n = e(X_n) = e(X/\nu_n Y_0) = e(X/Y_0) + e(Y_0/\nu_n Y_0)$. Comme $X/Y_0 = X_0$ est fini, le A -module Y_0 a les mêmes invariants ℓ et m que X , et en lui appliquant le théorème 8 du n° 6, on obtient le résultat cherché.

5. Structure de la p -extension abélienne non ramifiée maximale d'une Γ -extension. Cas général.

Revenons aux notations du début du n° 4, et soient $T_i = p^{n_i} \Gamma$ les groupes d'inertie des valuations de K qui se ramifient dans L . Choisissons un entier $n' \gg n_i$ pour tout i , et posons $K' = K_{n'}$. Le groupe de Galois Γ' de L/K' est isomorphe à \mathbb{Z} , et l'on peut appliquer à cette extension les résultats du numéro précédent. Le groupe X est donc un A' -module de type fini et de torsion, et a fortiori un A -module de type fini et de torsion. Le théorème 5 est donc valable sans modification, et un raisonnement analogue s'applique au théorème 6.

6. Structure de l'anneau Λ et des Λ -modules.

Soit $\Lambda = \mathbb{Z}_{\mathfrak{m}p}[[T]]$, et posons $\gamma = 1 - T$, $\gamma_n = \gamma^{p^n}$, $\omega_n = 1 - \gamma_n$. On a donc $\omega_0 = T$; l'idéal maximal \mathfrak{m} de Λ est l'idéal (p, T) . On voit facilement que le développement de ω_n est de la forme :

$$\omega_n = \sum_{i=1}^n a_i T^i + \sum_{i > n} a_i T^i, \text{ avec } i < p^n \text{ et } a_i \equiv 0 \pmod{p}.$$

Dans la terminologie des anneaux locaux, ω_n est un polynôme distingué (au signe près). Il s'ensuit que $\Lambda/\omega_n \Lambda$ s'identifie à $\mathbb{Z}_{\mathfrak{m}p}[T]/(\omega_n)$, anneau qui n'est autre que l'algèbre sur $\mathbb{Z}_{\mathfrak{m}p}$ du groupe cyclique $\mathbb{Z}/p^n \mathbb{Z}$, c'est-à-dire A_n avec les notations du n° 4. On a donc défini pour chaque entier n un homomorphisme surjectif $\Lambda \rightarrow A_n$, d'où, par passage à la limite un homomorphisme canonique

$$\xi: \Lambda \rightarrow A = \varprojlim A_n.$$

LEMME 3. - L'homomorphisme ξ est un isomorphisme.

Le noyau de ξ est l'intersection des $\omega_n \Lambda$. Or, si l'on pose :

$$\nu_n = 1 + \gamma_n + \gamma_n^2 + \dots + \gamma_n^{p-1},$$

on a évidemment $\nu_n \equiv 0 \pmod{\mathfrak{m}}$, et $\omega_{n+1} = \nu_n \omega_n$. Par récurrence on en conclut que $\omega_n \in \mathfrak{m}^n$, et $\bigcap \omega_n \Lambda \subset \bigcap \mathfrak{m}^n = 0$. Donc ξ est injectif; comme Λ et A sont tous deux compacts, et que l'image de ξ est dense dans A , ξ est bien un isomorphisme.

A partir de maintenant on identifiera Λ et A au moyen de ξ . On observera que l'anneau A est un anneau local régulier complet de dimension 2.

Soit X une limite projective de p -groupes finis munis de structures de $\mathbb{Z}_{\mathfrak{m}p}[\Gamma_n]$ -modules compatibles entre elles (cf. n° 4); comme on l'a déjà remarqué, ceci permet de définir sur X une structure de Λ -module topologique, évidemment compact.

LEMME 4. - Pour que X soit un Λ -module de type fini il faut et il suffit que $X/\mathfrak{m}X$ soit un p -groupe fini.

La nécessité est évidente. Supposons donc que des éléments $a_i \in X$, $1 \leq i \leq k$, engendrent X modulo $\mathfrak{m}X$, et soit Z le sous-module qu'ils engendrent; ce

sous-module est fermé, puisque c'est l'image continue de A^k , qui est compact. Dans $Y = X/Z$ on a $\mathfrak{m}Y = Y$; montrons que cette relation entraîne $Y = 0$, ce qui établira le lemme. Soit U un voisinage de 0 dans Y ; puisque Y est un A -module topologique, pour tout $y \in Y$ il existe un voisinage V_y de y et une puissance \mathfrak{m}^n de \mathfrak{m} tels que $\mathfrak{m}^n V_y \subset U$; par compacité on en déduit qu'il existe un n tel que $\mathfrak{m}^n Y \subset U$. Mais $\mathfrak{m}Y = Y$ entraîne $\mathfrak{m}^n Y = Y$; on a donc $Y \subset U$ pour tout U , d'où $Y = 0$ puisque Y est séparé.

REMARQUE. - Supposons que X soit de type fini. Alors sa topologie coïncide avec sa topologie \mathfrak{m} -adique; en effet, l'une est plus fine que l'autre, et toutes deux sont des topologies d'espace compact.

Nous allons maintenant nous occuper uniquement de A -modules de type fini, et donner un théorème de structure pour ces modules.

De façon générale, soit A un anneau noethérien intègre et intégralement clos, et soit \mathcal{C} la catégorie des A -modules de type fini dont l'annulateur n'est contenu dans aucun idéal premier de hauteur 1 de l'anneau A ; pour $A = \varprojlim_{\mathfrak{p}} [[T]]$ c'est la catégorie des A -modules qui sont des groupes finis.

On veut raisonner "modulo \mathcal{C} "; on dira donc qu'un homomorphisme $f : M \rightarrow M'$ est un \mathcal{C} -isomorphisme si son noyau et son conoyau appartiennent à \mathcal{C} ; définitions analogues pour \mathcal{C} -injectif et \mathcal{C} -bijectif.

D'autre part, on dira qu'un module M est réflexif s'il est égal à son bidual $M^{**} = \text{Hom}(\text{Hom}(M, A), A)$.

LEMME 5. - Pour tout A -module X de type fini, il existe un \mathcal{C} -isomorphisme $f : X \rightarrow X'$ où X' est somme directe d'un module réflexif et de modules de la forme A/\mathfrak{p}^n , où \mathfrak{p} est un idéal premier de hauteur 1 de A . De plus X' est déterminé de manière unique par X .

La démonstration est un simple exercice de localisation. Si T désigne le sous-module de torsion de X on commence par démontrer (en regardant la localisation de $\text{Hom}(X, T)$) qu'il existe un \mathcal{C} -isomorphisme de X dans $T \times X/T$, ce qui nous ramène aux deux cas suivants :

i. X est sans torsion. - On prend alors $X' = X^{**}$ et pour f l'application canonique $X \rightarrow X^{**}$; en localisant en \mathfrak{p} de hauteur 1, et en tenant compte de ce que $A_{\mathfrak{p}}$ est un anneau de valuation discrète on voit qu'on obtient un \mathcal{C} -isomorphisme.

ii. X est de torsion. - Chacun des $X_{\mathfrak{p}}$ est alors somme directe de modules de la forme $A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}$, et $X_{\mathfrak{p}} = 0$ pour presque tout \mathfrak{p} . D'où facilement le résultat.

La structure des modules réflexifs n'est pas facile à élucider dans le cas général. Heureusement, l'anneau $\mathbb{Z}_{\mathfrak{m}\mathfrak{p}}[[T]]$ est un anneau local régulier de dimension 2, et l'on peut appliquer le résultat suivant :

LEMME 6. - Si A est un anneau local régulier de dimension 2, tout A -module réflexif est libre.

Soit X un tel module ; on peut le plonger dans un module libre L de même rang, et dire que X est réflexif signifie que, dans la décomposition primaire de X dans L , les idéaux premiers qui interviennent sont de hauteur 1 (c'est essentiellement la "quasigleichheit" d'Artin, cf. par exemple [7], chapitre III, où est traité le cas des idéaux; celui des modules est identique). Avec les notations de [8], on a alors $\text{codh}(L/X) \geq 1$, d'où $\text{dh}(L/X) = \dim(A) - \text{codh}(L/X) \leq 1$; comme L est libre, on a $\text{dh}(X) = \text{dh}(L/X) - 1$, d'où $\text{dh}(X) \leq 0$, ce qui signifie que X est libre.

C. Q. F. D.

(L'analogie du lemme 6 pour les anneaux gradués redonne le théorème de Grothendieck sur les fibrés à fibre vectorielle de base la droite projective).

Les lemmes 5 et 6, appliqués à $A = \mathbb{Z}_{\mathfrak{m}\mathfrak{p}}[[T]]$ donnent le théorème de structure d'IWASAWA ([3], théorème 1) ; on doit seulement observer que les idéaux premiers de hauteur 1 de A sont de deux types (cf. [6], p. 60) :

- a. L'idéal $\mathfrak{p}A$ engendré par \mathfrak{p} .
- b. Un idéal engendré par un polynôme distingué irréductible :

$$F(T) = T^n + a_1 T^{n-1} + \dots + a_n, \quad a_i \equiv 0 \pmod{\mathfrak{p}}.$$

Dans le cas (a), le quotient A/\mathfrak{p}^n est simplement $\mathbb{Z}_{\mathfrak{m}\mathfrak{p}}/\mathfrak{p}^n \mathbb{Z}_{\mathfrak{m}\mathfrak{p}}[[T]]$. Dans le cas (b), c'est un $\mathbb{Z}_{\mathfrak{m}\mathfrak{p}}$ -module libre de type fini. On obtient donc finalement :

THÉOREME 7. - Soit \mathcal{C} la catégorie des A -modules de longueur finie. Tout A -module de type fini X est \mathcal{C} -isomorphe à une somme directe de modules qui sont, soit isomorphe à $\mathbb{Z}_{\mathfrak{m}\mathfrak{p}}[[T]]$, soit isomorphe à $\mathbb{Z}_{\mathfrak{m}\mathfrak{p}}/\mathfrak{p}^n \mathbb{Z}_{\mathfrak{m}\mathfrak{p}}[[T]]$, soit des $\mathbb{Z}_{\mathfrak{m}\mathfrak{p}}$ -modules libres de type fini.

De plus ces modules types sont déterminés par X de manière unique, à l'ordre près.

LEMME 7. - Soit X un A-module de type fini. Supposons que $X/\omega_n X$ soit un \mathbb{Z}_p -module de type fini dont le rang reste borné quand $n \rightarrow +\infty$. Alors X est un module de torsion.

On voit tout de suite que l'hypothèse est invariante par \mathbb{C} -isomorphisme. On peut donc supposer que X est somme directe des modules types énumérés dans le théorème 7, et tout revient à voir que le rang de $A/\omega_n A$ n'est pas borné. Or $A/\omega_n A$ est l'algèbre sur \mathbb{Z}_p du groupe Γ_n , et son rang sur \mathbb{Z}_p est p^n qui tend vers l'infini avec n.

C. Q. F. D.

Si X est un A-module de torsion de type fini, on définit ses invariants m et ℓ comme on l'a expliqué à la fin du n° 4.

THÉOREME 8. - Soit X un A-module de type fini, et supposons que pour tout entier n, $X/\nu_n X$ soit un groupe fini, d'ordre p^{en} . Le module X est alors un module de torsion, et si m et ℓ sont ses invariants on a :

$$(*) \quad e_n = mp^n + \ell n + c \text{ pour } n \text{ grand, } c \text{ étant une constante.}$$

Ici encore, la question est invariante par \mathbb{C} -isomorphisme, et l'on est ramené aux trois cas suivants :

i. $X = A$. - Dans ce cas $X/\nu_n X$ n'est pas un groupe fini, contrairement à l'hypothèse.

ii. $X = A/p^m A$. - On écrit la suite exacte :

$$X/\omega_0 X \xrightarrow{\nu_n} X/\omega_n X \longrightarrow X/\nu_n X \longrightarrow 0,$$

et comme $X/\omega_n X = \mathbb{Z}_p^m[\Gamma_n]$, on a $e(X/\omega_n X) = mp^n$, d'où $e(X/\nu_n X) = mp^n - c$ pour n grand.

iii. X est un \mathbb{Z}_p -module libre de rang ℓ . - La structure de Γ -module de X est définie par l'automorphisme associé à γ , c'est-à-dire par une matrice carrée M, de degré ℓ , à coefficients dans \mathbb{Z}_p ; pour que cette opération définisse sur X une structure de A-module il est nécessaire et suffisant que M soit unipotente mod p, c'est-à-dire qu'une puissance de (M - 1) soit $\equiv 0 \pmod p$. Pour n assez grand, on aura $\gamma_n \equiv 1 \pmod p$, d'où $\gamma_{n+1} \equiv 1 \pmod{p^2}$

Si l'on pose $\nu'_n = 1 + \gamma_n + \gamma_n^2 + \dots + \gamma_n^{p-1}$, on en déduit $\nu'_n \equiv p \pmod{p^2}$,

c'est-à-dire $\nu'_n = p \cdot u_n$, où u_n est inversible. Comme $\nu_n = \nu'_n \nu_{n-1}$, on a donc $\nu_n X = p \nu_{n-1} X$ pour $n \geq n_0$, d'où $\nu_n X = p^{n-n_0} \nu_{n_0} X$ si $n \geq n_0$. On en tire, en posant $Y = \nu_{n_0} X$:

$$e(X/\nu_n X) = e(X/Y) + e(Y/p^{n-n_0} Y) = c_1 + \ell(n - n_0) ,$$

puisque Y a même rang sur $\mathbb{Z}_{\neq p}$ que X , d'où le résultat cherché.

BIBLIOGRAPHIE

- [1] HASSE (Helmut). - Über die Klassenzahl Abelscher Zahlkörper. - Berlin, Akademie Verlag, 1952.
- [2] IWASAWA (Kenkichi). - A note on class numbers of algebraic number fields, Abh. math. Sem. Hamburg, t. 20, 1956, p. 257-258.
- [3] IWASAWA (Kenkichi). - On Γ -extensions of algebraic number fields, Bull. Amer. math. Soc., t. 65, 1959 (à paraître).
- [4] IWASAWA (Kenkichi). - On some invariants of cyclotomic fields, Amer. J. of Math., t. 80, 1958, p. 773-783.
- [5] IWASAWA (Kenkichi). - Sheaves for algebraic number fields, Annals of Math., Series 2, t. 69, 1959, p. 408-413.
- [6] SAMUEL (Pierre). - Algèbre locale. - Paris, Gauthier-Villars, 1953 (Mém. Sc. math., 123).
- [7] SAMUEL (Pierre). - Commutative algebra (Notes by D. Hertzig). - Ithaca, Cornell University, 1953.
- [8] SERRE (Jean-Pierre). - Sur la dimension homologique des anneaux et des modules noethériens, Proc. intern. Symp. on alg. number theory [1955. Tokyo et Nikko]. - Tokyo, Science Council of Japan, 1956 ; p. 175-189.