L. BOUVIER

J. J. PAYAN

Modules sur certains anneaux de Dedekind

Séminaire de théorie des nombres de Grenoble, tome 2 (1972-1973), exp. n° 3, p. 1-12

<http://www.numdam.org/item?id=STNG_1972-1973__2__A3_0>

Exposé de J.J. PAYAN d'après un travail avec L. BOUVIER
9 et 16 novembre 1972

MODULES SUR CERTAINS ANNEAUX DE DEDEKIND

La structure des modules de type fini sur un anneau de Dedekind est bien connue et on sait les renseignements que divers auteurs en ont tirés sur la structure de certains invariants arithmétiques (voir notamment [4], [5], [6] et [11]). Le but du présent travail est de simplifier la démonstration de certains résultats connus (voir notamment [9]), voire d'en étendre la portée. Rappelons les deux énoncés suivants (voir [2]) :

Théorème A.

Soit A un anneau de Dedekind et soit M un A-module de type fini et de torsion, alors il existe une famille finie d'idéaux premiers $\mathfrak{p}_i$ de A et d'entiers $n_i \geq 1$ tel que M soit isomorphe à $\bigoplus_{i \in I} A/\mathfrak{p}_i^{n_i}$.

Théorème B.

Soit A un anneau de Dedekind et soit M un A-module de type fini, sans torsion et de rang $n \geq 1$, alors il existe un idéal $\mathfrak{a}$ non nul de A tel que M soit isomorphe à $A^{n-1} \oplus \mathfrak{a}$.

I - PRELIMINAIRES ALGEBRIQUES.

Soit G un groupe cyclique d'ordre p^n, p premier, engendré par σ. Notons A_n l'anneau des entiers du corps $\mathbb{Q}^{(p^n)}$ des racines p^n-ièmes de l'unité.

<u>Proposition 1.</u>

$\mathbb{Z}[G]/(1+\sigma^{p^{n-1}}+\ldots+\sigma^{(p-1)p^{n-1}})$ <u>est isomorphe à</u> A_n .

Il suffit pour le voir de considérer l'homomorphisme φ de $\mathbb{Z}[G]$ dans A_n défini par $\varphi(\sigma) = \zeta_n$ où ζ_n est une racine primitive p^n-ième de l'unité, et d'utiliser l'égalité $A_n = \mathbb{Z}[\zeta_n]$ d'une part et, de l'autre, le fait que $1 + X^{p^{n-1}}+\ldots+ X^{(p-1)p^{n-1}}$ est le polynôme cyclotomique d'indice p^n .

<u>Théorème 1.</u>

<u>Soit</u> M <u>un</u> $\mathbb{Z}[G]$-<u>module de type fini et sans torsion sur</u> $\mathbb{Z}$. <u>Notons</u> M' (<u>resp.</u> M_o) <u>le sous-</u>$\mathbb{Z}[G]$-<u>module formé des éléments de</u> M <u>annulés par</u> $1 + \sigma^{p^{n-1}}+\ldots+ \sigma^{(p-1)p^{n-1}}$ (<u>resp.</u> $1-\sigma^{p^{n-1}}$) , <u>alors</u> M' <u>et</u> M/M_o <u>sont des</u> A_n-<u>modules de type fini, sans torsion et isomorphes. Si de plus</u> M <u>est monogène,</u> M' <u>et</u> M/M_o <u>sont libres sur</u> A_n <u>et de rang</u> 1 .

<u>Démonstration</u> : Les $\mathbb{Z}[G]$-modules M' et M/M_o sont des $\mathbb{Z}[G]$-modules annulés par $1 + \sigma^{p^{n-1}}+\ldots+ \sigma^{(p-1)p^{n-1}}$, donc, via la proposition 1, ce sont des A_n-modules. Comme ils sont de type fini sur $\mathbb{Z}$, ils sont de type fini sur A_n . Le $\mathbb{Z}$-module M' est trivialement sans torsion et M_o est facteur direct du $\mathbb{Z}$-module M , il en résulte que M/M_o est aussi sans $\mathbb{Z}$-torsion. Reprenons le raisonnement de [6], page 4, pour montrer que M' et M/M_o sont sans torsion sur A_n :

Soient $\alpha \in M'$ (resp. $\alpha \in M/M_o$) avec $\alpha \neq 0$ et $\lambda \in A_n$ tels que $\lambda\alpha = 0$. Désignons par $\lambda_1,\lambda_2,\ldots,\lambda_{(p-1)p^{n-1}}$ les conjugués de λ dans $\mathbb{Q}^{(p^n)}/\mathbb{Q}$, on a $(\lambda_1\lambda_2\ldots\lambda_{(p-1)p^{n-1}})\alpha = N_{\mathbb{Q}^{(p^n)}/\mathbb{Q}}(\lambda).\alpha = 0$. Or $N_{\mathbb{Q}^{(p^n)}/\mathbb{Q}}(\lambda)\in\mathbb{Z}$, donc $N_{\mathbb{Q}^{(p^n)}/\mathbb{Q}}(\lambda) = 0$ et, par suite, $\lambda = 0$.

Notons que $M'\cap M_o = \{0\}$ et remarquons que les suites

$$0 \to M' \to M \to (1+\sigma^{p^{n-1}}+\ldots+\sigma^{(p-1)p^{n-1}})M \to 0$$

et

$$0 \to M' \to M'\oplus M_o \to pM_o \to 0$$

sont exactes et que $pM_o \subset (1+\sigma^{p^{n-1}}+\dots+\sigma^{(p-1)p^{n-1}})M \subset M_o$.

Il en résulte que $M/M'\oplus M_o$ et $(1+\sigma^{p^{n-1}}+\dots+\sigma^{(p-1)p^{n-1}})M/pM_o$ sont isomorphes, donc les $\mathbb{Z}$-rangs de M et de $M'\oplus M_o$ sont égaux ainsi que les $\mathbb{Z}$-rangs de M/M_o et de M' .

En outre, l'application de M' dans M/M_o qui à $\alpha \in M'$ fait correspondre $\alpha + M_o$ est un homomorphisme injectif de A_n-module et on a M/M_o / $M'\oplus M_o/M_o$ isomorphe à $M/M'\oplus M_o$, lui-même isomorphe à $(1+\sigma^{p^{n-1}}+\dots+\sigma^{(p-1)p^{n-1}})M/pM_o$ qui est un A_n-module de torsion. Et on a

$$\mathrm{Cl}\ M/M_o = \mathrm{Cl}\,M' \times \mathrm{Cl}\,(1+\sigma^{p^{n-1}}+\dots+\sigma^{(p-1)p^{n-1}})M/pM_o) \ ,$$

or l'idéal premier au-dessus de p dans A_n est principal donc $\mathrm{Cl}((1+\sigma^{p^{n-1}}+\dots+\sigma^{(p-1)p^{n-1}})M/pM_o) = 1$, ce qui termine la démonstration de la première partie du théorème.

Supposons maintenant M monogène, $M = \mathbb{Z}[G]\theta$, il est alors clair que la classe $\tilde{\theta}$ de θ modulo M_o engendre M/M_o comme A_n-module ; or M/M_o est sans torsion sur A_n , on a donc $M/M_o = A_n\bar{\theta}$.

Soit maintenant G le groupe défini par les générateurs σ et τ et les relations $\sigma^p = \tau^m = 1$ et $\tau\sigma\tau^{-1} = \sigma^r$ où p est un nombre premier impair, m un entier diviseur de $p-1$ et r une racine primitive m-ième de l'unité modulo p . On note alors $H = \{1,\sigma,\dots,\sigma^{p-1}\}$ et $\bar{g} = \{1,\tau,\dots,\tau^{m-1}\}$ Le groupe $\bar{g}$ opère fidèlement sur H par "automorphismes intérieurs" et il y a $\frac{p-1}{m}+1$ orbites : l'une est réduite à un élément et les autres ont m éléments. A chacune de ces dernières est associé un entier i_ℓ $(\ell=1,2,\dots,\frac{p-1}{m})$ tel que l'orbite soit formée des éléments $\sigma^{i_\ell r^t}$, t entier variant de 0 à $m-1$, on pose $T_\ell = \sum_{t=0}^{m-1} \sigma^{i_\ell r^t}$. Considérons la sous-algèbre $\mathfrak{a}$ de $\mathbb{Z}[H]$ engendrée par l'élément neutre et les T_ℓ et notons $A_{(m)}$ l'anneau des entiers du corps intermédiaire de $\mathbb{Q}^{(p)}/\mathbb{Q}$ de degré $\frac{p-1}{m}$ sur $\mathbb{Q}$.

On obtient alors la proposition suivante, donnée par J. Martinet dans le cas diédral (cf. [12]), par J. Cougnard dans le cas $m = q$ premier et étendue par N. Moser au cas m quelconque :

Proposition 2.

$\mathfrak{a}/(1+\sigma+\ldots+\sigma^{p-1})$ est isomorphe à $A_{(m)}$.

Pour s'en convaincre, il suffit de considérer l'homomorphisme φ de $\mathfrak{a}$ dans $A_{(m)}$ défini par

$$\varphi(T_\ell) = \sum_{t=0}^{m-1} \zeta^{i_\ell r^t}$$

où ζ est une racine primitive p-ième de l'unité.

II - STRUCTURES MULTIPLICATIVES.

1. Groupe des classes. On désigne par $\mathcal{K}$ un corps de nombres.

a - Cas cyclique relatif. Soit $K = K_n$ une extension cyclique de degré p^n de $\mathcal{K}$ avec p premier et n entier ≥ 1 . On pose $G = \mathrm{Gal}\, K/\mathcal{K}$ et on note σ un générateur de G et K_i ; l'extension intermédiaire de $K/\mathcal{K}$ de degré p^i avec $i \in \{1,2,\ldots,n\}$.

Soient $\mathcal{H}_n^*$ le groupe des classes relatives de K_n sur K_{n-1} et h_n^* le cardinal de $\mathcal{H}_n^*$.

Théorème.

Le A_n-module $\mathcal{H}_n^*$ est isomorphe à $\bigoplus_{i\in I} A_n/\mathfrak{p}_i^{n_i}$ où I est fini, les $\mathfrak{p}_i$ sont des idéaux premiers et les n_i des entiers ≥ 1 .

On montre simplement que $\mathcal{H}_n^*$ est un A_n-module grâce à la proposition I et, comme $\mathcal{H}_n^*$ est fini, l'énoncé résulte du théorème A .

Corollaire.

h_n^* est norme sur $\mathbb{Q}$ d'un idéal de A_n .

En effet, $h_n^* = N_{K/\mathbb{Q}}(\prod_{i\in I} \mathfrak{p}_i^{n_i})$. Par exemple, si on prend pour K le corps de conducteur 89 et de degré 8 sur $\mathbb{Q}$, $h^* = 113$ et $13 = N_{\mathbb{Q}(8)/\mathbb{Q}}((1+\sqrt{2}+2i\sqrt{2}))$.

Remarque II.1 : Le théorème 2.1 de [9] donne l'énoncé du corollaire dans le cas $\mathcal{X} = \mathbb{Q}$. Françoise Bertrandias nous a, par ailleurs, fait observer qu'une légère adaptation de la méthode qu'elle a exposée dans [1] livre également le résultat de ce corollaire.

Remarque II.2 : Si p ne divise pas le nombre de classe de $\mathcal{X}$ et si un idéal fini et un seul se ramifie dans $K_1/\mathcal{X}$, alors on sait, d'après Iwasawa (voir [8]), que p ne divise pas le nombre de classe h_n de K_n et on peut écrire $\mathcal{H}_{K_n} = \mathcal{H}^*_{K_n} \oplus \mathcal{H}_{K_{n-1}}$ où $\mathcal{H}_{K_i}$ représente le groupe des classes des idéaux de K_i. On en déduit $h^*_n \equiv 1 \ (p^n)$. En particulier si $\mathcal{X} = \mathbb{Q}$, si le conducteur de $K_n/\mathbb{Q}$ est primaire et si K_{n-1} est principal alors $h_n \equiv 1 \ (p^n)$. Cette dernière assertion trouve de nombreuses illustrations dans les tables de [7].

b - Cas pm : $K/\mathcal{X}$ désigne maintenant une extension de degré p premier dont la clôture galoisienne $N/\mathcal{X}$ a un groupe de Galois $\mathrm{Gal}\, N/\mathcal{X}$ dont le p-sous-groupe de Sylow est distingué. Il est alors facile de montrer (cf. [3]) que, si K est non galoisienne, $\mathrm{Gal}\, N/\mathcal{X}$ est isomorphe au groupe G intervenant dans la proposition 2. On identifiera ces deux groupes en supposant que $\mathrm{Gal}\, N/K$ est engendré par τ. On notera k le corps intermédiaire qui appartient à H et $\mathcal{H}_K$ le groupe des classes relatives de K sur $\mathcal{X}$.

Lemme.

Le groupe $\mathcal{F}_K$ des idéaux fractionnaires non nuls de K est un G-module.

Il suffit de montrer que si $\mathfrak{p}$ est un idéal premier de K, $\mathfrak{p}^{T_\ell} \in \mathcal{F}_K$ pour $\ell = 1, 2, \ldots, \frac{p-1}{m}$, c'est-à-dire, en désignant par A_N l'anneau des entiers de N, que $(\mathfrak{p}A_N)^{T_\ell} = \mathfrak{b}A_N$ avec $\mathfrak{b} \in \mathcal{F}_K$.

Or $\mathfrak{p}A_N = \left(\prod_{j=0}^{g-1} \mathfrak{P}_j\right)^{\ell}$ où les $\mathfrak{P}_j$ sont des idéaux premiers distincts de A_N, de degré f sur K avec $m = efg$, leur groupe de décomposition est le sous-groupe de $\mathrm{Gal}\, N/K$ engendré par τ^g. Posons pour tout entier

$j \geq 0$, $\mathfrak{P}_{[j]} = \mathfrak{P}_0^{\tau^j}$ avec $[j] \in \{0,1,\dots,g-1\}$ et $[j] \equiv j$ (modulo g). Alors

$$(\mathfrak{p}A_N)^{T_\ell} = \Big(\prod_{j=0}^{g-1} \mathfrak{P}_{[j]}^{T_\ell}\Big)^e ,$$

or $\mathfrak{P}_{[j]}^{T_\ell} = \prod_{k=0}^{m-1} \mathfrak{P}_{[j]}^{\tau^k \sigma^{i_\ell} \tau^{-k}} = \prod_{k=0}^{m-1} \mathfrak{P}_{[j-k]}^{\tau^k \sigma^{i_\ell}}$ et, pour k fixé, lorsque j parcourt $\{0,1,\dots,g-1\}$ il en est de même pour $[j-k]$. Donc

$$(\mathfrak{p}A_N)^{T_\ell} = \Big(\prod_{k=0}^{m-1}\Big(\prod_{j=0}^{g-1} \mathfrak{P}_{[j]}^{\sigma^{i_\ell}}\Big)^{\tau^k}\Big)^e = N_{N/K}\Big(\prod_{j=0}^{g-1}\mathfrak{P}_{[j]}^{\sigma^{i_\ell}}\Big) A_N .$$

On peut alors énoncer le

Théorème 2.

Le $A_{(m)}$-module $\mathcal{H}_K$ est isomorphe à $\bigoplus_{i\in I} A_{(m)}/\mathfrak{q}_i^{n_i}$ où les $\mathfrak{q}_i$ forment une famille finie d'idéaux premiers de $A_{(m)}$ et où les n_i sont des entiers ≥ 1.

Démonstration : En désignant par $\mathcal{P}_K$ le sous-groupe des idéaux principaux de $\mathcal{F}_K$, $\mathcal{P}_K$ est un G-module puisque K^* est un G-module (voir par exemple [5]), $\mathcal{F}_K/\mathcal{P}_K$ ainsi que $\mathcal{H}_K$ sont aussi des G-modules. On en déduit facilement que $\mathcal{H}_K$, qui est annulé par $1 + \sigma + \dots + \sigma^{p-1}$ est un $A_{(m)}$-module, de plus il est fini et on obtient le résultat en appliquant le théorème A.

2. Groupe des unités.

On se limite au cas d'une extension K cyclique de degré p^n sur $\mathbb{Q}$ (p premier), que l'on suppose réelle si $p = 2$.

On note encore K_i l'extension intermédiaire de $K/\mathbb{Q}$ de degré p^i avec $0 \leq i \leq n$ et σ un générateur de $G = \mathrm{Gal}\, K/\mathbb{Q}$

$$\begin{array}{c} K = K_n \\ \Big| \; p \\ K_{n-1} \\ \vdots \\ K_1 \\ \Big| \; p \\ \mathbb{Q} \end{array}$$

Pour $i \in \{1,2,\ldots,n\}$, on désigne par $U^{+}_{K_i}$ le groupe des unités de K_i de norme 1 sur $\mathbb{Q}$, par $U^{*}_{K_i}$ le groupe des unités relatives de K_i sur K_{i-1} , c'est-à-dire de norme 1 sur K_{i-1} ,et, pour U_{K_i} le groupe des unités de K_i . Dans le cas $p = 2$, on fait le quotient par $\{\pm 1\}$ pour avoir des $\mathbb{Z}$-modules sans torsion.

<u>Lemme</u>.

$U^{*}_{K_n}$ <u>est un A_n-module de type fini et sans torsion</u>.

Il est clair que $U^{*}_{K_n}$ est un $\mathbb{Z}[G]/(1+\sigma^{p^{n-1}}+\ldots+\sigma^{(p-1)p^{n-1}})$-module , donc, grâce à la proposition I, un A_n-module. On montre comme dans [6] qu'il est sans torsion puisqu'il est sans torsion sur $\mathbb{Z}$.

On peut remarquer que le rang de $U^{*}_{K_n}$ sur A_n est égal à 1 . En effet, en utilisant le théorème de Dirichlet d'une part et le fait que $U^{*}_{K_n}$ est le noyau de l'application norme de U_{K_n} dans $U_{K_{n-1}}$ dont l'image est d'indice fini dans $U_{K_{n-1}}$ de l'autre, on montre que $U^{*}_{K_n}$ et A_n ont même rang sur $\mathbb{Z}$. D'où,via le théorème B la

<u>Proposition 3</u>.

$U^{*}_{K_n}$ <u>est isomorphe à un idéal</u> $\mathfrak{a}$ <u>de</u> A_n .

On dit que ε est une unité de Minkowski (resp. une unité de Minkowski relative) de K_i ($i \in \{1,2,\ldots,n\}$) si $\varepsilon \in U^{+}_{K_i}$ (resp. $\varepsilon \in U^{*}_{K_i}$) et si $U^{+}_{K_i} = \varepsilon^{\mathbb{Z}[G]}$ (resp. $U^{*}_{K_i} = \varepsilon^{\mathbb{Z}[G]}$) . D'après la proposition précédente, on obtient :

<u>Proposition 4</u>.

<u>Si</u> A_n <u>est principal</u>, <u>il existe alors une unité de Minkowski relative à chaque</u> "<u>étage</u>", <u>c'est-à-dire une unité de Minkowski relative de</u> K_i <u>pour tout</u> $i \in \{1,2,\ldots,n\}$.

Rappelons au passage l'énoncé de Brummer (cf. [4]) qui concerne le cas $n = 1$, Proposition.

Le groupe H des unités cyclotomiques est A_1-libre, donc H est isomorphe à A_1. On prolonge cet isomorphisme à U_{K_1} et on en déduit que U_{K_1} est isomorphe à $\mathfrak{a}^{-1}$ où $\mathfrak{a}$ est un idéal entier de A_1, que le nombre h de classes de K_1 vérifie $h = [U_{K_1}:H] = N_{\mathbb{Q}^{(p)}/\mathbb{Q}}\,\mathfrak{a}$ et qu'il existe une unité de Minkowski si tous les idéaux entiers de norme h sont principaux.

Les unités cyclotomiques généralisées introduites par H.W. Leopoldt dans [9] doivent permettre une généralisation complète de l'énoncé de Brummer dans le cas cyclique relatif. Dans le cas particulier où tous les idéaux premiers ramifiés de $K/\mathbb{Q}$ sont totalement ramifiés, en notant H_{K_i} (resp. $H^*_{K_i}$) le groupe des unités cyclotomiques de K_i (resp. des unités cyclotomiques relatives de K_i sur K_{i-1}) pour $i = n$ ou $n-1$, $h_{K_i} = [U_{K_i}:H_{K_i}]$, en posant $h^*_K = \dfrac{h_{K_n}}{h_{K_{n-1}}}$ et en supposant en outre, que $H^*_{K_n}$ est $\mathbb{Z}[G]$-monogène, on montre alors

Proposition 5.

<u>Pour qu'il existe une unité de Minkowski relative de</u> K, <u>il suffit que tous les idéaux de norme</u> h^*_K <u>soient principaux</u>.

Pour qu'il existe une unité de Minkowski de K, il est nécessaire qu'il existe une unité de Minkowski relative à chaque "étage" et que l'application norme de $U^+_{K_i}$ dans $U^+_{K_{i-1}}$ soit surjective pour tout $i \in \{1,2,..,n\}$. Ce qui nous amène à formuler la conjecture suivante que nous avons vérifiée dans certains cas particuliers :

> " si A_n est principal et si, pour tout $i \in \{1,2 \ldots,n\}$, l'application norme de $U^+_{K_i}$ sur $U^+_{K_{i-1}}$ est surjective, alors il existe une unité de Minkowski de K".

Remarque : Il y a d'autres groupes multiplicatifs associés à K dont on peut faire des $\mathbb{Z}[G]$-modules, comme par exemple, le groupe des S-unités où S est un ensemble fini de places de K stable par G.

III - STRUCTURES ADDITIVES.

Soit K une extension cyclique de degré p^n de $\mathbb{Q}$ avec p premier et n entier ≥ 1, et soit K_o l'extension intermédiaire de degré p^{n-1} sur $\mathbb{Q}$. On désigne par A_K (resp. A_{K_o}) l'anneau des entiers de K (resp. K_o) et par A_K^* l'anneau des entiers relatifs de K, c'est-à-dire de trace nulle sur K_o.

Par une démonstration analogue à celle faite pour les unités relatives de K, on montre que A_K^* est un A_n-module sans torsion de rang 1, de plus il est isomorphe à A_K/A_{K_o}.

En utilisant l'application trace Tr de K sur K_o, on voit que $A_K/A_K^* \oplus A_{K_o}$ est isomorphe à $\operatorname{Tr} A_K/pA_{K_o}$. On en déduit que $A_K^* \oplus A_{K_o}$ est un sous-$\mathbb{Z}$-module de type fini de A_K et même :

Proposition 6.

Le quotient $A_K/A_K^* \oplus A_{K_o}$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{fg(e-r)}$ où $r = \frac{(t+1)(p-1)}{p}$, $pA_{K_o} = (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_g)^e$, $\operatorname{Tr} A_K = (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_g)^r$, les $\mathfrak{p}_i$ sont des idéaux premiers de K_o et t est le nombre de ramification associé aux $\mathfrak{p}_i$ dans K/K_o et A_K^* est isomorphe à un idéal non nul de A_n.

Si $e = r$, on a alors $A_K = A_{K_o} \oplus A_K^*$, ce qui se produit notamment lorsque :

- $n = 1$ et (p) est ramifié dans K
- $K/\mathbb{Q}$ a pour conducteur une puissance de p.

Lorsque $n = 1$ et (p) non ramifié dans K, $A_K = \mathbb{Z}[G]$ avec $G = \operatorname{Gal} K/\mathbb{Q}$ et $\mathbb{Z} \oplus A_K^*$ est d'indice p dans A_K ; $A_K/\mathbb{Z}$ est alors libre sur A_1 et, par suite, A_K^* est libre sur A_1. Lorsque $n = 1$ et (p) ramifié dans $K/\mathbb{Q}$, on sait directement que A_K^* est libre sur A_1 (base quasi-normale).

Lorsque $K/\mathbb{Q}$ a comme conducteur une puissance de p, $A_K = \mathbb{Z} \oplus A_{K_1}^* \oplus \ldots \oplus A_{K_n}^*$ où $A_{K_i}^*$ désigne l'anneau des entiers relatifs de l'extension intermédiaire K_i de degré p^i sur $\mathbb{Q}$ sur l'extension intermédiaire de degré p^{i-1} sur $\mathbb{Q}$, $i \in \{1,2,\ldots,n\}$. On peut alors se demander si les

$A^*_{K_i}$ sont libres sur l'anneau A_i correspondant. Les résultats de Leopoldt-Jacobinski (cf. [10]) devraient donner une réponse positive.

IV - APPLICATIONS AUX Γ-EXTENSIONS.

Soit K_∞ une Γ-extension d'un corps de nombres $\mathcal{K}$, c'est-à-dire une extension galoisienne de $\mathcal{K}$ dont le groupe de Galois soit isomorphe à $\mathbb{Z}_p$. Notons K_n l'extension intermédiaire de $K_\infty/\mathcal{K}$ de degré p^n sur $\mathcal{K}$, $\mathfrak{H}_{K_n}$ (resp. $\mathfrak{H}^*_{K_n}$) le groupe des classes de K_n (resp. des classes relatives de K_n sur K_{n-1}), $\mathfrak{H}_\infty$ le groupe des classes d'idéaux de type fini de K_∞ et $\mathfrak{H}_{\mathcal{K}}$ le groupe des classes de $\mathcal{K}$.

On suppose vérifier les hypothèses suivantes :

a) p ne divise pas le nombre de classes de $\mathcal{K}$

b) p est divisible par un seul idéal de $\mathcal{K}$ et se ramifie dans $K_1/\mathcal{K}$.

Proposition 7.

$\mathfrak{H}_\infty$ est isomorphe à $\mathfrak{H}_{\mathcal{K}} \overset{\infty}{\underset{i=1}{\oplus}} \prod_{i\in I_n} A_n/\mathfrak{a}_{n,i}$ où les $\mathfrak{a}_{n,i}$ forment une famille finie d'idéaux entiers de A_n.

Démonstration : Cela résulte immédiatement du théorème d'Iwasawa (cf. [8]) disant que sous les hypothèses ci-dessus $\mathfrak{H}_{K_n}$ est d'ordre premier à p d'où $\mathfrak{H}_\infty = \mathfrak{H}_{\mathcal{K}} \overset{\infty}{\underset{i=1}{\oplus}} \mathfrak{H}_{K_n}$ et du théorème 2.

Remarque : Bien que sous les hypothèses précédentes, l'application norme soit une surjection du groupe des unités de K_n sur le groupe des unités de K_{n-1}, on n'a pas d'écriture agréable pour les unités de K_∞.

En ce qui concerne la structure additive, nous supposons maintenant que $\mathcal{K} = \mathbb{Q}$ on peut alors énoncer la

Proposition 8.

$A_{K_\infty} = \mathbb{Z} \overset{\infty}{\underset{i=1}{\oplus}} A^*_{K_n}$ c'est-à-dire $A_{K_\infty} = \mathbb{Z} \overset{\infty}{\underset{i=1}{\oplus}} \mathfrak{a}_n$ où $\mathfrak{a}_n$ est un idéal entier de A_n et en désignant par A_{K_∞} (resp. $A^*_{K_n}$) l'anneau des entiers de K_∞ (resp. l'anneau des entiers relatifs de K_n).

Démonstration : La seconde assertion se déduit de la première en appliquant la proposition 4. La première assertion résulte de la première partie de la proposition 4 compte tenu de ce que p est totalement ramifié et que $t = \frac{p^n-1}{p-1}$ (voir [14] pour son calcul explicite).

BIBLIOGRAPHIE

[1] - F. BERTRANDIAS - "Sur le nombre de classes relatif d'une extension cyclique de degré ℓ^ν (ℓ premier impair) de corps de nombres". Séminaire de Théorie des Nombres. Grenoble - 1972.

[2] - N. BOURBAKI - "Algèbre commutative" Chap.VII. Hermann, Paris (1961).

[3] - L. BOUVIER - "Construction de certaines extensions de degré p". Séminaire de Théorie des Nombres. Grenoble. 1972.

[4] - A. BRUMER - "On the group of units of an absolutely cyclic number field of prime degree". J. Math. Soc. Japan. Vol.21. n°3 - 1969.

[5] - J. COUGNARD - "Sur les extensions galoisiennes non abéliennes de degré pq du corps des rationnels (p et q premiers)". C.R.A.S. 274 A (1972), pp. 936-939 et Thèse de 3e cycle.

[6] - G. GRAS - "Etude du groupe des unités d'un anneau d'entiers algébriques dans le cas galoisien cyclique". Séminaire de Théorie des Nombres. Grenoble. 1969.

[7] - H. HASSE - "Uber Die Klassenzahl Abelscher Zahlkörper". Akademie-Verlag Berlin (1952).

[8] - K. IWASAWA - "A note on class numbers of algebraic number fields". Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg - Band 20, Heft 3/4 (1956) pp. 257-258.

[9] - H.W. LEOPOLDT - "Uber Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper". Abh. d. D.A.W. - 1953 - 2 - pp. 1-48.

[10] - H.W. LEOPOLDT - "Uber die Hauptordnung des ganze Elemente eines abelschen Zahlkörper". J. reine angew. Math.201 (1959) pp. 119-149.

[11] - J. MARTINET - "Anneau des entiers d'une extension galoisienne considéré comme module sur l'algèbre du groupe de Galois". Bull. Soc. Math. France, Mémoire 25 - 1971 - pp. 123-126.

[12] - J. MARTINET - "Sur l'algèbre des extensions galoisiennes à groupe de Galois diédral d'ordre 2p". Thèse. Chap.I §2 et 3 .

[13] - J.J. PAYAN - "Contribution à l'étude des corps abéliens absolus de degré premier impair". Thèse - Chap.III - Théorème 8. Annales de l'Institut Fourier XV 2 (1965) pp. 133-199.

[14] - J.P. SERRE - "Corps locaux". Hermann. Paris (1962).
