ANNALES DE L'INSTITUT FOURIER

FRANÇOISE BERTRANDIAS

Décomposition du Galois-module des entiers d'une extension cyclique de degré premier d'un corps de nombres ou d'un corps local

Annales de l'institut Fourier, tome 29, n° 1 (1979), p. 33-48

<http://www.numdam.org/item?id=AIF_1979__29_1_33_0>

Ann. Inst. Fourier, Grenoble
29, 1 (1979), 33-48

DECOMPOSITION DU GALOIS-MODULE DES ENTIERS D'UNE EXTENSION CYCLIQUE DE DEGRÉ PREMIER D'UN CORPS DE NOMBRES OU D'UN CORPS LOCAL

par Françoise BERTRANDIAS

Dédié à Monsieur Claude Chabauty.

Soit A un anneau de Dedekind, de corps des fractions K, et soit L une extension galoisienne finie de K, de groupe de Galois G. La clôture intégrale B de A dans L est un A[G]-module de rang 1 ; B est somme directe d'un nombre fini de sous A[G]-modules indécomposables et, lorsque G est abélien, cette décomposition est unique ; elle a été déterminée, dans le cas où K est le corps $\mathbf{Q}$ des rationnels, par H.W. Leopoldt [6].

On se propose ici de trouver la décomposition de B lorsque G est un groupe cyclique de degré premier, et K un corps local ou un corps de nombres algébriques.

On étudie d'abord la décomposition d'un A[G]-module de rang 1, lorsque G est abélien (§ 1), puis lorsque G est cyclique de degré premier et K est un corps local ou un corps de nombres (§ 2). Le cas du Galois-module B est traité dans le § 3 lorsque K est un corps local, et dans le § 4 lorsque K est un corps de nombres.

1. Décomposition d'un A[G]-module de rang 1.

1.1. Décomposition et idempotents.

On désigne par :

A un anneau commutatif intègre de corps des fractions K,
G un groupe fini,
M un A[G]-module, de type fini et sans torsion sur A,
$C(M) = \mathrm{End}_{A[G]}M$ le commutant de M.

On sait qu'il existe des décompositions de M en somme directe de sous-A[G]-modules indécomposables (utiliser par exemple le fait que l'application canonique de M dans $K \otimes_A M$ est injective).

Rappelons les relations entre les décompositions en somme directe d'un module M et les idempotents de son commutant C(M). Soit une décomposition en somme directe de sous-A[G]-modules :

$$M = \bigoplus_{1 \leqslant i \leqslant k} M_i \tag{1}$$

et soit $e_i : M \longrightarrow M_i$ la projection canonique $(1 \leqslant i \leqslant k)$. Alors $(e_i)_{1 \leqslant i \leqslant k}$ est un système d'idempotents complet orthogonal de C(M), c'est-à-dire :

$$\begin{cases} 1_{C(M)} = \sum_{1 \leqslant i \leqslant k} e_i \\ e_i e_j = \delta_{i,j} . \end{cases} \tag{2}$$

Réciproquement, à tout système d'idempotents complet orthogonal de C(M) correspond la décomposition de M en somme directe :

$$M = \bigoplus_{1 \leqslant i \leqslant k} e_i M .$$

Un idempotent non nul de C(M) est dit primitif si l'égalité : $e = e' + e''$ où e' et e'' sont deux idempotents orthogonaux de C(M), entraîne : $e' = 0$ ou $e'' = 0$.

Un sous-module M figurant dans la décomposition (1) de M est indécomposable si, et seulement si, l'idempotent correspondant e_i est primitif.

On voit donc que trouver une décomposition de M en somme directe de sous-A[G]-modules indécomposables revient à trouver un système complet orthogonal d'idempotents primitifs de C(M). (On notera fréquemment : système d'idempotents c.o.p.)

1.2. Commutant et ordre associé.

Rappelons les définitions suivantes ([7]) : un A[G]-module M est de rang 1 si M est de type fini et sans torsion sur A, et si le K[G]-module $K \otimes_A M$ est libre avec un générateur. L'ordre associé à un K[G]-module M de rang 1 est le sous-anneau de K[G] défini par : $\mathfrak{O}(M) = \{\lambda \in K[G] \mid \lambda M \subset M\}$.

On montre facilement :

PROPOSITION 1. – *Soit* G *un groupe abélien et soit* M *un* A[G]*-module de rang* 1. *L'application qui à un élément* λ *de* $\mathfrak{O}(M)$, *associe la multiplication à gauche par* λ *dans* M, *est un isomorphisme d'anneaux de* $\mathfrak{O}$ (M) *sur* C(M).

Pour trouver les décompositions de M, on est donc ramené à chercher les systèmes complets orthogonaux d'idempotents primitifs de $\mathfrak{O}$ (M).

1.3. Unicité de la décomposition.

On suppose G abélien et M de rang 1.

PROPOSITION 2. –

1) *Il existe un unique système* S *complet orthogonal d'idempotents primitifs dans* $\mathfrak{O}$ (M).

2) S *est l'ensemble des idempotents primitifs de* $\mathfrak{O}$ (M).

Démonstration. – L'existence de S provient de l'existence de décompositions du module M en somme directe de sous-modules indécomposables (§ 1.1). L'unicité de S, et le fait que tout idempotent primitif de $\mathfrak{O}$ (M) soit contenu dans S, proviennent du lemme suivant (dont la démonstration est analogue à celle du lemme 5.7 de [10], ch. 3) :

LEMME. – *Soit* R *un anneau commutatif possédant un système* S *complet orthogonal d'idempotents primitifs. Alors* S *est l'ensemble des idempotents primitifs de* R.

La proposition 2 entraîne immédiatement :

PROPOSITION 3. – *Soit* G *un groupe abélien et* M *un* A[G]*-module de rang* 1. *Si* S *est l'ensemble des idempotents primitifs de* $\mathfrak{O}$ (M), *la décomposition :* $M = \bigoplus_{e \in S} eM$ *est l'unique décomposition de* M *en somme directe de sous* A[G]*-modules indécomposables.*

1.4. Idempotents de K[G].

Rappelons comment s'obtiennent les idempotents de K[G] (cf. [3]). On suppose le groupe G abélien et le corps K de carac-

téristique 0. Soit I l'ensemble des caractères irréductibles de G sur K. Pour tout χ appartenant à I, on pose :

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g .$$

On a les résultats suivants :

(1) e_χ est un idempotent primitif de K[G], et K[G] e_χ est un corps ;

(2) on a la décomposition : $K[G] = \bigoplus_{\chi \in I} K[G]\, e_\chi$;

(3) $(e_\chi)_{\chi \in I}$ est l'ensemble des idempotents primitifs de K[G].

On montre facilement :

PROPOSITION 4. — *Tout idempotent e de* K[G] *s'écrit :* $e = \sum_{\chi \in J} e_\chi$, J *étant un ensemble de caractères irréductibles de* G *sur* K.

Remarque. — Soit n l'exposant de G, et soit $\mathbf{Q}^{(n)}$ le corps engendré sur $\mathbf{Q}$ par les racines n-èmes de 1. Les valeurs prises par un caractère χ de G appartiennent à $\mathbf{Q}^{(n)}$. Par suite, les idempotents e_χ, et donc aussi tous les idempotents de K[G], appartiennent à l'algèbre $\mathbf{Q}^{(n)}[G]$.

2. Cas où G cyclique de degré premier, et K corps local ou corps de nombres.

Hypothèses et notations.

G est un groupe cyclique de degré premier p.

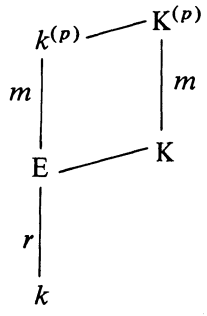
K est un corps local (de caractéristique 0 et de caractéristique résiduelle p) ou un corps de nombres, et A l'anneau de ses entiers.

M est un A[G]-module de rang 1.

On pose : $k = \begin{cases} \mathbf{Q}_p & \text{si K est un corps local,} \\ \mathbf{Q} & \text{si K est un corps de nombres.} \end{cases}$

($\mathbf{Q}_p$ désignant le corps des nombres p-adiques).

2.1. Les caractères irréductibles de G sur K.



Notons, dans une clôture algébrique de k, $k^{(p)}$ (resp. $K^{(p)}$) le corps engendré sur k (resp. K) par les racines p-èmes de 1 et $E = K \cap k^{(p)}$.

Soit $X^p - 1 = (X-1)\,P_1(X) \ldots P_r(X)$ la décomposition du polynôme $X^p - 1$ en produit de polynômes irréductibles de K[X]. Les polynômes $P_i(X)$, $(1 \leqslant i \leqslant r)$, ont tous le même degré m et l'on a : $m = [K^{(p)} : K] = \dfrac{p-1}{r}$. De plus, l'extension $k^{(p)}/E$ étant galoisienne, $[k^{(p)} : E] = [K^{(p)} : K] = m$. Par suite, les polynômes $P_i(X)$, $(1 \leqslant i \leqslant r)$, appartiennent à E[X]. On a les isomorphismes de K-algèbres :

$$K[G] \cong K[X]/X^p - 1 \cong K[X]/(X-1) \times \\ \times K[X]/P_1(X) \times \ldots \times K[X]/P_r(X).$$

Le groupe G possède donc $r+1$ représentations irréductibles sur K : 1 représentation de degré 1, et r représentations de degré m. Comme les polynômes $P_i(X)$ appartiennent à E[X], les $r+1$ représentations de G proviennent, par extension des scalaires, des $r+1$ représentations irréductibles de G sur E. Pour tout caractère irréductible χ de G sur K, l'idempotent e_χ appartient donc à E[G] (cf. remarque du § 1.4).

Notations.

On note :

χ_0 le caractère de la représentation de degré 1,

χ_i, $(1 \leqslant i \leqslant r)$, le caractère de la représentation $K[X]/P_i(X)$,

$T = \sum_{g \in G} g$,

$e_{\chi_0} = T/p$.

2.2. Action du groupe de Galois de l'extension E/k.

L'extension E/k est cyclique de degré r, et $\mathrm{Gal}(E/k)$ opère sur l'ensemble des représentations irréductibles de G sur E, et donc aussi sur leurs caractères. On voit facilement que χ_0 est invariant, et que les caractères χ_i $(1 \leqslant i \leqslant r)$ sont permutés transitivement.

En posant, pour tout φ de $\mathrm{Gal}(E/k)$ et pour tout $\lambda = \sum_{g \in G} a_g g$ de $E[G]$: $\varphi\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} \varphi(a_g) g$, on obtient une opération de $\mathrm{Gal}(E/k)$ sur $E[G]$; φ est un automorphisme de k-algèbre de $E[G]$.

On remarque que le groupe $\mathrm{Gal}(E/k)$ laisse invariant l'idempotent e_{χ_0} et permute transitivement les idempotents e_{χ_i} $(1 \leqslant i \leqslant r)$.

2.3. Hypothèse d'invariance.

Soit M un A[G]-module de rang 1, et $\mathfrak{O}(M)$ son ordre associé dans K[G]. On sait que tout idempotent de $\mathfrak{O}(M)$ appartient à E[G]. On supposera par la suite que l'ordre $\mathfrak{O}(M)$ vérifie l'hypothèse suivante :

HYPOTHESE D'INVARIANCE (H). — *Tout élément de* $\mathrm{Gal}(E/k)$ *laisse globalement invariant l'ordre* $\mathfrak{O}(M) \cap E[G]$.

THEOREME 1. — *Soit* M *un* A[G]*-module de rang* 1 *décomposable, dont l'ordre associé* $\mathfrak{O}(M)$ *vérifie l'hypothèse d'invariance* (H). *Soit* F *le plus petit corps intermédiaire entre* k *et* E *tel que* F[G] *contienne tous les idempotents de* $\mathfrak{O}(M)$. *Alors* F[G] *et* $\mathfrak{O}(M)$ *ont les mêmes idempotents.*

Démonstration. — Notons :

S l'ensemble des idempotents primitifs de $\mathfrak{O}(M)$,
$r_F = [F : k]$,
τ un générateur du groupe cyclique $\mathrm{Gal}(F/k)$.

D'après le choix du corps F, il existe un idempotent e de S tel que les éléments $\tau^i(e)$, $(0 \leqslant i < r_F)$, soient tous distincts. Ces éléments $\tau^i(e)$ appartiennent à $\mathfrak{O}(M)$ (hypothèse (H)), et sont nécessairement des idempotents primitifs de $\mathfrak{O}(M)$. Soit

$e' = 1 - \sum_{0 \leqslant i < r_F} \tau^i(e)$; e' est un idempotent et $(e', e, \tau(e), \ldots, \tau^{r_F - 1}(e))$ est un système complet orthogonal d'idempotents de $\mathfrak{O}(M)$. Comme ce système a le même nombre d'éléments, $r_F + 1$ que le système d'idempotents c.o.p. S' de $F[G]$, il ne peut que coïncider avec S' et donc aussi avec S.

2.4. Modules décomposables.

Le théorème 1 entraîne immédiatement :

PROPOSITION 5. – *Soit* M *un* A[G]*-module dont l'ordre associé* $\mathfrak{O}(M)$ *vérifie l'hypothèse d'invariance* (H). M *est décomposable si et seulement si l'idempotent* T/p appartient à $\mathfrak{O}(M)$. *Dans ce cas, on a la décomposition :*

$$M = \frac{T}{p} M \oplus \left(1 - \frac{T}{p}\right) M .$$

Remarque. – L'idempotent T/p est primitif dans $K[G]$, et donc aussi dans $\mathfrak{O}(M)$. Par suite, le module $\frac{T}{p} M$ est indécomposable.

3. Anneau des entiers d'une extension cyclique de degré premier d'un corps local.

Notations et hypothèses.

K est un corps local de caractéristique 0 et de caractéristique résiduelle p, d'anneau de valuation A ;
L est une extension cyclique de degré p de K ;
B est l'anneau des entiers de L ;
σ est un générateur de $G = \mathrm{Gal}(L/K)$;
t est le nombre de ramification de l'extension L/K.

B est un A[G]-module de rang 1. On se propose de trouver la décomposition de B en somme directe de sous-A[G]-modules indécomposables.

3.1. L'ordre associé à B.

Si l'extension L/K est non ramifiée, $\mathfrak{O}(B) = A[G]$ (cf. [9]). Si l'extension est ramifiée, $\mathfrak{O}(B)$ a été déterminé précédemment

([1], [2], [4]). Pour énoncer le résultat, introduisons les notations et définitions suivantes ; *pour tout réel* x :

$[x]$ est le plus grand entier inférieur ou égal à x,
$\underset{\smile}{x} = x - [x]$ est la partie fractionnaire de x,
$\mathfrak{E}(x) = \{h$ entier $\geqslant 1 \mid h'$ entier et $1 \leqslant h' < h$ entraînent : $\underset{\smile}{h'x} > \underset{\smile}{hx}\}$.

Si K *est un corps local :*

v_K désigne la valuation normalisée de K,
e_K désigne l'indice absolu de ramification de K.

PROPOSITION 6. – *Soit, pour tout entier* i $(0 \leqslant i \leqslant p-1)$, $n_i = \left[\frac{it}{p}\right] + \delta_i$, *où* $\delta_i = \begin{cases} 1 \text{ si } p - i \in \mathfrak{E}(t/p) \\ 0 \text{ sinon} \end{cases}$. *On a :*

$$\mathfrak{D}(B) = \left\{ \sum_{0 \leqslant i \leqslant p-1} a_i(\sigma - 1)^i \mid a_i \in K \text{ et } v_K(a_i) \geqslant -n_i \ (0 \leqslant i \leqslant p-1) \right\}.$$

On en déduit facilement :

PROPOSITION 7. – *L'ordre* $\mathfrak{D}$ (B) *vérifie l'hypothèse d'invariance* (H).

3.2. Modules B décomposables.

THEOREME 2. – *Le* A[G]*-module* B *est décomposable si, et seulement si, l'une des conditions équivalentes suivantes est vérifiée :*

(1) *l'idempotent* T/p *appartient à* $\mathfrak{D}$ (B) ;

(2) *le nombre de ramification* t *de l'extension* L/K *est tel que :*

$$\frac{p}{p-1} e_K - 1 \leqslant t \leqslant \frac{p}{p-1} e_K .$$

DEFINITION. – *Le nombre de ramification* t *de l'extension* L/K *est dit "presque maximal"* (cf. [5]) *si l'une ou l'autre des conditions équivalentes* (1) *ou* (2) *est vérifiée.*

Démonstration. – L'ordre $\mathfrak{D}$ (B) vérifie l'hypothèse d'invariance (H). Donc (proposition 5) B est décomposable si, et seulement si, T/p appartient à $\mathfrak{D}$ (B). L'équivalence des conditions (1) et (2) résulte facilement de la description de l'ordre $\mathfrak{D}$ (B) (cf. [4]).

Ce théorème a été démontré précédemment, et indépendamment, par M.J. Ferton (1975, non publié) et Y. Miyata [8].

3.3. Décomposition de B. Enoncé des résultats.

Notations.

a désigne le reste de la division de t par p ;
I désigne l'ensemble des caractères irréductibles de G sur K.

THEOREME 3. – *Soit* L/K *une extension cyclique de degré* p *de corps locaux dont le nombre de ramification* t *est presque maximal.*

1) *Si* a *est nul ou divise* $p-1$, *l'ensemble des idempotents primitifs de* $\mathfrak{D}$ (B) *est* $\{e_\chi \mid \chi \in I\}$ *et la décomposition de* B *en somme directe de sous-modules indécomposables s'écrit* : $B = \bigoplus_{\chi \in I} e_\chi B$.

2) *Si* a *est différent de* 0 *et ne divise par* $p-1$, *l'ensemble des idempotents primitifs de* $\mathfrak{D}$ (B) *est* $\left\{ \frac{T}{p}, 1 - \frac{T}{p} \right\}$ *et la décomposition de* B *en somme directe de sous-modules indécomposables s'écrit* : $B = \frac{T}{p} B \oplus \left(1 - \frac{T}{p}\right) B$.

Remarque. – Un A[G]-module N, de type fini sans torsion sur A, est A-irréductible si $K \otimes_A N$ est un K[G]-module simple (cf. [3]). Pour tout $\chi \in I$, $e_\chi B$ est A-irréductible. En particulier $\frac{T}{p} B$ est A-irréductible. Par contre, $\left(1 - \frac{T}{p}\right) B$ est A-irréductible si et seulement si les corps K et $\mathbf{Q}_p^{(p)}$ sont linéairement disjoints sur $\mathbf{Q}_p$ ($r = 1$). Le théorème 3 montre donc que B est décomposable en somme directe de sous-A[G]-modules A-irréductibles si et seulement si

1) t est presque maximal
2) ou bien K et $\mathbf{Q}_p^{(p)}$ sont linéairement disjoints sur $\mathbf{Q}_p$ ou bien a est nul ou divise $p-1$.

3.4. Démonstration du théorème 3.

D'après le théorème 1, l'ensemble S des idempotents primitifs de $\mathfrak{D}(M)$ coïncide avec l'ensemble des idempotents primitifs de F[G], où F est le plus petit corps intermédiaire entre $\mathbf{Q}_p$ et E

tel que F[G] contienne S. Il s'agit donc de déterminer le corps F. La démonstration se fait en plusieurs étapes.

On vérifie immédiatement le

LEMME 1. — F *est le plus grand corps intermédiaire entre* $\mathbf{Q}_p$ *et* E *tel que, pour tout caractère irréductible* χ *de* G *sur* F, e_χ *appartient à* $\mathfrak{D}$ (B).

Introduisons les notations suivantes : A_F est l'anneau des entiers de F, $\mathfrak{M}_F$ l'ordre maximal de l'algèbre F[G] ; $e(K/F) = e_K/e_F$; $m_F = [\mathbf{Q}_p^{(p)} : F]$.

On montre facilement le

LEMME 2. — *Soit* F *un corps local contenu dans* $\mathbf{Q}_p^{(p)}$. *Alors* $\mathfrak{M}_F$ *est l'anneau engendré par* $A_F[G]$ *et par les idempotents* e_χ, χ *parcourant l'ensemble des caractères irréductibles de* G *sur* F.

Par ailleurs, on démontre le

LEMME 3. — *Pour tout corps local* F, *on a*

$$\mathfrak{M}_F = \left\{ \sum_{0 \leqslant i \leqslant p-1} a_i(\sigma - 1)^i \mid a_i \in F \text{ et } v_F(a_i) \geqslant -\left[\frac{i}{p-1} e_F \right] \right\}.$$

LEMME 4. — F *est le plus grand corps intermédiaire entre* $\mathbf{Q}_p$ *et* E *tel que, pour tout entier* i, $0 \leqslant i \leqslant p-1$, *on ait :*

$$e(K/F) \underbrace{\frac{i}{m_F}} - \underbrace{\frac{ia}{p}} - \frac{ia}{p(p-1)} + \delta_i \geqslant 0 \qquad (1)$$

où δ_i *vaut* 1 *ou* 0 *suivant que* $p - i$ *appartient à* $\mathscr{E}\left(\frac{t}{p}\right)$ *ou non.*

Démonstration. — Les lemmes 1, 2, 3 et la description de l'ordre $\mathfrak{D}$(B) (proposition 6) entraînent : F est le plus grand corps intermédiaire entre $\mathbf{Q}_p$ et E tel que $\frac{n_i}{e(K/F)} \geqslant \left[\frac{i}{p-1} e_F \right]$, $(0 \leqslant i \leqslant p-1)$. Posons : $t = a + up$, $(0 \leqslant a \leqslant p-1)$. Comme t est presque maximal, on a (cf. [4]) : $e_K = a + u(p-1)$. On en déduit (remarquer que $p - 1 = e_F m_F$) :

$$n_i - e(K/F)\left[\frac{i}{p-1} e_F \right] = e(K/F) \underbrace{\frac{i}{m_F}} - \underbrace{\frac{ia}{p}} - \frac{ia}{p(p-1)} + \delta_i .$$

Le lemme 4 en résulte.

LEMME 5. – *Si* $a = 0$, *on a* : $F = E$. *Si* $a \neq 0$, F *est le plus grand corps intermédiaire entre* $\mathbf{Q}_p$ *et* E *tel que l'ensemble des entiers* $\{p - jm_F \mid 1 \leqslant j \leqslant e_F\}$ *soit contenu dans* $\mathcal{E}\left(\frac{t}{p}\right)$.

Démonstration. – Si $a = 0$, l'inégalité (1) est vérifiée pour tout corps intermédiaire F entre $\mathbf{Q}_p$ et E. Supposons $a \neq 0$. Soit F un corps intermédiaire entre $\mathbf{Q}_p$ et E, et soit i un entier non multiple de m_F. On a :

$$e(K/F)\,\underbrace{\frac{i}{m_F}} - \frac{ia}{p(p-1)} \geqslant \frac{a}{p-1} - \frac{ia}{p(p-1)} \geqslant 0$$

et donc (1) est vérifiée. Le lemme 5 en résulte.

LEMME 6. – *Soit* d *un diviseur de* $p-1$, $d < p-1$. *Les entiers* $p - jd$, $1 \leqslant j \leqslant \frac{p-1}{d}$, *appartiennent à* $\mathcal{E}\left(\frac{t}{p}\right)$ *si et seulement si* a *divise* $p-1$ *et* $\frac{p-1}{a}$ *divise* d.

Démonstration. – On utilise le développement en fraction continue de t/p, en notant $q_0 = 1$, $q_1, \ldots, q_i = a_i q_{i-1} + q_{i-2}, \ldots, q_n = p$, les dénominateurs des réduites de t/p (on suppose $a_n > 1$). On montre ([4]) :

$$\mathcal{E}\left(\frac{t}{p}\right) = \{p\} \cup \left\{ q_{2i} + xq_{2i+1} \mid 0 \leqslant i < \frac{n-1}{2} \text{ et } x \text{ entier}, \right.$$
$$\left. 0 \leqslant x \leqslant a_{2i+2} \right\}.$$

Supposons que $p - d$ *et* $p - 2d$ *appartiennent à* $\mathcal{E}\left(\frac{t}{p}\right)$; il existe des entiers i, j, x, y tels que :

$$p - d = q_{2i} + xq_{2i+1}\ ,\quad 0 \leqslant j \leqslant i < \frac{n-1}{2}$$

$$p - 2d = q_{2j} + yq_{2j+1}\ ,\quad 0 \leqslant x \leqslant a_{2i+2}\ ,\quad 0 \leqslant y \leqslant a_{2j+2}\ .$$

On en déduit : $p = 2(q_{2i} + xq_{2i+1}) - (q_{2j} + yq_{2j+1}) < 2q_{2i+2}$. Comme $p = a_n q_{n-1} + q_{n-2} > 2q_{n-1}$, on a : $2i + 2 > n - 1$, et donc $2i = n - 2$. Par suite $p = a_{2i+2} q_{2i+1} + q_{2i}$, et $d = (a_{2i+2} - x)q_{2i+1}$. Ceci entraîne : q_{2i+1} divise d et donc divise $p - 1$. On en déduit : q_{2i+1} divise $q_{2i} - 1$ et donc $q_{2i} = 1$. D'où $i = 0$, et $n = 2$. Il en résulte : a *divise* $p - 1$, $a \neq 1$. Posons $q = \frac{p-1}{a}$; on a $q_1 = q$ et $a_2 = a$. D'où :

$$\mathcal{E}\left(\frac{t}{p}\right) = \{1 + xq \mid x \text{ entier et } 0 \leqslant x \leqslant a\}$$
$$= \{p - jq \mid j \text{ entier et } 0 \leqslant j \leqslant a\}.$$

On en déduit le résultat annoncé.

On peut alors terminer la démonstration du théorème 3. Si $a = 0$, on a vu que $F = E$. *Supposons donc* $a \neq 0$. Si F est un corps intermédiaire entre $\mathbf{Q}_p$ et E, m_F est un multiple de $m = m_E$, et $F = \mathbf{Q}_p$ si et seulement si $m_F = p - 1$. *Si a ne divise pas* $p - 1$, les lemmes 5 et 6 montrent que $m_F = p - 1$, d'où $F = \mathbf{Q}_p$. *Si a divise* $p - 1$, pour tout corps F intermédiaire entre $\mathbf{Q}_p$ et E, $\frac{p-1}{a}$ divise m_F ; en effet, $m_F = \frac{p-1}{a}\frac{a}{e_F}$, et e_F, divisant e_K et $p - 1$, divise $a = e_K - u(p-1)$. Par suite, si $a = 1$, $m_F = p - 1$, et donc $F = E = \mathbf{Q}_p$. Si $a \neq 1$, pour tout corps F intermédiaire entre $\mathbf{Q}_p$ et E, $\{p - jm_F \mid 1 \leqslant j \leqslant e_F\}$ est contenu dans $\mathcal{E}\left(\frac{t}{p}\right)$, d'après le lemme 6. D'où $F = E$ (lemme 5).

On en déduit le théorème 3.

4. Anneau des entiers d'une extension cyclique de degré premier d'un corps de nombres.

Notations et hypothèses.

K est un corps de nombres, A son anneau d'entiers,
L une extension cyclique de degré p de K,
B l'anneau des entiers de L,
σ est un générateur de $G = \mathrm{Gal}(L/K)$.

B est un A[G]-module de rang 1 ; on se propose de déterminer la décomposition de B en somme directe de sous-modules indécomposables.

4.1. Les extensions $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.

Pour tout idéal premier $\mathfrak{P}$ de L, on note :

$L_{\mathfrak{P}}$ un complété de L pour la valuation $\mathfrak{P}$-adique ;
$B_{\mathfrak{P}}$ l'anneau des entiers de $L_{\mathfrak{P}}$; $\mathfrak{p} = \mathfrak{P} \cap A$;
$K_{\mathfrak{p}}$ le complété de K dans $L_{\mathfrak{P}}$ pour la valuation $\mathfrak{p}$-adique ;

$A_\mathfrak{p}$ l'anneau des entiers de $K_\mathfrak{p}$;

$v_\mathfrak{P}$ (resp. $v_\mathfrak{p}$) la valuation $\mathfrak{P}$ -adique (resp. $\mathfrak{p}$ -adique) normalisée de $L_\mathfrak{P}$ (resp. $K_\mathfrak{p}$).

La factorisation de $\mathfrak{p}B$ en idéaux premiers de L a l'une des 3 formes suivantes :

a) $\mathfrak{p}B = \mathfrak{P}^p$ ($\mathfrak{p}$ ramifié)

b) $\mathfrak{p}B = \mathfrak{P}$ ($\mathfrak{p}$ inerte)

c) $\mathfrak{p}B = \mathfrak{P}\ \sigma\mathfrak{P} \ldots \sigma^{p-1}\mathfrak{P}$ ($\mathfrak{p}$ décomposé).

Dans les cas a) ou b), $L_\mathfrak{P}/K_\mathfrak{p}$ est une extension cyclique de degré p ; on identifie son groupe de Galois à G. On note $t_\mathfrak{p}$ le nombre de ramification de l'extension $L_\mathfrak{P}/K_\mathfrak{p}$. Si l'idéal $\mathfrak{p}$ est au-dessus de p, et se ramifie dans L, l'extension $L_\mathfrak{P}/K_\mathfrak{p}$ est sauvagement ramifiée. On connait, d'après l'étude locale du § 3, les idempotents de l'ordre $\mathfrak{O}(B_\mathfrak{P})$, ordre associé à $B_\mathfrak{P}$ dans l'algèbre $K_\mathfrak{p}[G]$. Dans le cas c), on a $L_\mathfrak{P} = K_\mathfrak{p}$.

4.2. L'ordre $\mathfrak{O}(B)$.

PROPOSITION 8. — *Soit* $n_{\mathfrak{p},i}$ *l'entier défini pour tout idéal premier* $\mathfrak{p}$ *de* K, *et pour tout entier* i, $0 \leqslant i \leqslant p-1$, *par* $n_{\mathfrak{p},i} = 0$, *sauf si* $\mathfrak{p}$ *est sauvagement ramifié dans* L, *auquel cas on pose :*

$$n_{\mathfrak{p},i} = \left[\frac{i}{p}\, t_\mathfrak{p}\right] + \delta_i, \quad \textit{avec} \quad \delta_i = \begin{cases} 1 & \textit{si} \quad p - i \in \mathfrak{E}\left(\frac{t}{p}\right) \\ 0 & \textit{sinon} \end{cases}.$$

L'ordre $\mathfrak{O}(B)$ *est donné par :*

$$\mathfrak{O}(B) = \left\{ \sum_{0 \leqslant i \leqslant p-1} a_i(\sigma - 1)^i \mid a_i \in K \textit{ et } v_\mathfrak{p}(a_i) \geqslant -n_{\mathfrak{p},i}, \textit{ pour tout idéal premier } \mathfrak{p} \textit{ de } K, \textit{ et tout entier } i, \ 0 \leqslant i \leqslant p-1 \right\}$$

Démonstration. — Soit $\lambda = \sum_{0 \leqslant i \leqslant p-1} a_i(\sigma - 1)^i$ un élément de $K[G]$; λ appartient à $\mathfrak{O}(B)$ si et seulement si, pour tout $\mathfrak{P}$ idéal premier de L, on a :

$$\text{pour tout } x \text{ appartenant à } B, \quad v_\mathfrak{P}(\lambda x) \geqslant 0. \tag{1}$$

Si $\mathfrak{P} \cap A$ *n'est pas décomposé dans* L, on voit facilement que (1) équivaut à : λ appartient à $\mathfrak{O}(B_\mathfrak{P})$; par suite, (1) équivaut à $v_\mathfrak{p}(a_i) \geqslant -n_{\mathfrak{p},i}$ d'après l'étude locale (proposition 6).

Si $\mathfrak{P} \cap A$ *est décomposé dans* L, on montre, en utilisant par exemple le théorème des restes chinois relatif à l'anneau A et aux idéaux $\sigma^i\mathfrak{P}$, que (1) équivaut à : $v_{\mathfrak{p}}(a_i) \geqslant 0$, pour tout entier i, $0 \leqslant i \leqslant p-1$.

De la proposition 8, on déduit :

PROPOSITION 9. – *L'ordre* $\mathfrak{O}$ (B) *vérifie l'hypothèse d'invariance* (H).

4.3. Modules B décomposables.

On déduit facilement des résultats antérieurs :

THEOREME 4. – *Le* A[G]*-module* B *est décomposable si et seulement si l'une des deux conditions équivalentes suivantes est vérifiée :*

(1) *l'idempotent* T/p *appartient à* $\mathfrak{O}$(B),

(2) *tout idéal premier* $\mathfrak{p}$ *de* K *au-dessus de* p *est ramifié dans* L, *et le nombre de ramification correspondant* $t_{\mathfrak{p}}$ *est presque maximal, c'est-à-dire :* $\dfrac{p}{p-1}\, e_K - 1 \leqslant t_{\mathfrak{p}} \leqslant \dfrac{p}{p-1}\, e_K$.

4.4. Décomposition de B.

Notations.

Soit I l'ensemble des caractères irréductibles de G sur K ; notons $a_{\mathfrak{p}}$ le reste de la division de $t_{\mathfrak{p}}$ par p.

THEOREME 5. – *Soit* L/K *une extension cyclique de degré* p *de corps de nombres telle que tout idéal premier* $\mathfrak{p}$ *de* K *au-dessus de* p *soit ramifié dans* L, *le nombre de ramification correspondant* t *étant presque maximal.*

1) *Si, pour tout* $\mathfrak{p}$ *au-dessus de* p, $a_{\mathfrak{p}}$ *est nul ou divise* $p-1$, *l'ensemble des idempotents primitifs de* $\mathfrak{O}$(B) *est* $\{e_\chi \mid \chi \in I\}$, *et la décomposition de* B *en somme directe de sous-*A[G]*-modules indécomposables s'écrit :* $B = \bigoplus_{\chi \in I} e_\chi B$.

2) *S'il existe un idéal premier* $\mathfrak{p}$ *de* K *au-dessus de* p *tel que* $a_{\mathfrak{p}} \neq 0$, *et* $a_{\mathfrak{p}}$ *ne divise pas* $p-1$, *l'ensemble des idempotents primitifs de* $\mathfrak{O}$(B) *est* $\left\{ \dfrac{T}{p}, 1 - \dfrac{T}{p} \right\}$ *et la décomposition de* B

*en somme directe de sous-*A[G]*-modules indécomposables s'écrit :*
$B = \frac{T}{p} B \oplus \left(1 - \frac{T}{p}\right) B$.

Démonstration. – Elle se déduit facilement de l'étude locale (théorème 3) et du fait qu'un idempotent e de K[G] appartient à $\mathfrak{O}(B)$ si et seulement si, pour tout $\mathfrak{P}$ au-dessus de p, e appartient à $\mathfrak{O}(B_{\mathfrak{P}})$.

Remarque. – (cf. remarque du § 3.3) B est décomposable en somme directe de sous A[G]-modules A-irréductibles si, et seulement si

1) tout idéal premier $\mathfrak{p}$ de K au-dessus de p est ramifié dans L, et le nombre de ramification $t_{\mathfrak{p}}$ correspondant est presque maximal ;

2) ou bien K et $\mathbf{Q}^{(p)}$ sont linéairement disjoints sur $\mathbf{Q}$, ou bien, pour tout $\mathfrak{p}$ au-dessus de p, $a_{\mathfrak{p}}$ est nul ou divise $p-1$.

BIBLIOGRAPHIE

[1] F. BERTRANDIAS et M.J. FERTON, Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local, *C.R. Acad. Sc.*, Paris, 274 (1972), 1330-1333.

[2] F. BERTRANDIAS, J.P. BERTRANDIAS et M.J. FERTON, Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local, *C.R. Acad. Sc.*, Paris, 274 (1972), 1388-1391.

[3] C.W. CURTIS et I. REINER, Representation theory of finite groups and associative algebras, *Pure and Appl. Math.*, XI, Interscience, New York, (1962).

[4] M.J. FERTON, Sur l'anneau des entiers d'extensions cycliques de degré p et d'extensions diédrales de degré $2p$ d'un corps local, *Thèse de doctorat de troisième cycle,* Grenoble, (1972).

[5] H. JACOBINSKI, Uber die Hauptordnung eines Körpers als Gruppen modul, *J. reine angew. Math.*, 213 (1964), 151-164.