

ANNE-MARIE BERGÉ

**Arithmétique d'une extension galoisienne
à groupe d'inertie cyclique**

Annales de l'institut Fourier, tome 28, n° 4 (1978), p. 17-44

http://www.numdam.org/item?id=AIF_1978__28_4_17_0

© Annales de l'institut Fourier, 1978, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.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/>

ARITHMÉTIQUE D'UNE EXTENSION GALOISIENNE A GROUPE D'INERTIE CYCLIQUE

par Anne-Marie BERGÉ ⁽¹⁾

Soit K un corps de nombres, et soit L une extension galoisienne finie de K . Notons G le groupe de Galois de L/K . D'après le théorème de la base normale, L est un module libre sur l'algèbre de groupe $K[G]$, avec un générateur. Notons A et B les anneaux entiers de K et L . D'après ce qui précède, B est un $A[G]$ -module de rang 1, et nous savons que, pour que B soit localement libre sur $A[G]$, il faut et il suffit que l'extension L/K soit modérément ramifiée (voir [4]). Lorsque l'extension n'est pas modérément ramifiée, on introduit l'ensemble $\mathfrak{D} = \{\lambda \in K[G] / \lambda B \subset B\}$. C'est un ordre de A dans $K[G]$, et B est un \mathfrak{D} -module de rang 1. Dans cet article, nous étudions l'ordre \mathfrak{D} et la structure locale de B comme \mathfrak{D} -module (l'ordre \mathfrak{D} est évidemment le seul sur lequel B puisse être localement libre), pour certains types de groupes G et de corps K , mais sans hypothèses restrictives sur la ramification. Nous confrontons souvent nos résultats au théorème global démontré par Leopoldt pour les extensions abéliennes du corps \mathbb{Q} des rationnels (voir [3], et aussi [2]): l'ordre \mathfrak{D} est l'algèbre sur \mathbb{Z} engendrée par $\mathbb{Z}[G]$ et les idempotents

$$e_H = \frac{1}{\text{card } H} \sum_{s \in H} s,$$

où H parcourt les sous-groupes supérieurs de ramification des idéaux premiers de B . De plus, B est libre sur \mathfrak{D} .

(1) Laboratoire associé au C.N.R.S. n° 226.

Nous désignons désormais par K un corps local de caractéristique 0 et de caractéristique résiduelle $p \neq 0$. Nous supposons K absolument non ramifié (i.e. $\nu_K(p) = 1$). Nous considérons une extension galoisienne finie L/K de groupe de Galois G . Nous notons G_0 et L_0 le groupe et le corps d'inertie. Nous supposons G_0 cyclique sauf dans le paragraphe 1 où sont rassemblés des résultats généraux relatifs à la ramification. Dans le paragraphe 2, nous donnons une description explicite de l'ordre \mathfrak{D} . Notre méthode consiste à se ramener aux ordres associés à B dans les algèbres $K[G_0]$ et $L_0[G_0]$, grâce à un résultat de Jacobinski ([2]). La comparaison de ces ordres fournit dans le paragraphe 3 des conditions nécessaires (portant sur la ramification) pour que B soit libre sur \mathfrak{D} . Nous appliquons ces résultats à la construction explicite d'une extension de \mathbb{Q} (évidemment non abélienne, et sauvagement ramifiée), dont l'anneau d'entiers n'est pas localement libre sur son ordre associé \mathfrak{D} . Enfin, nous caractérisons, dans le paragraphe 4, les extensions cycliques totalement ramifiées de K pour lesquelles B est libre sur \mathfrak{D} , par une condition sur la ramification. Nous montrons en particulier que, sauf lorsque $K = \mathbb{Q}_p$, il existe des extensions cycliques de K pour lesquelles N n'est pas libre sur \mathfrak{D} .

Les méthodes exposées dans cet article permettent d'obtenir pour les extensions diédrales des résultats complets qui feront l'objet d'un article ultérieur.

1. RAMIFICATION

Nous notons G_i les sous-groupes de ramification de G . En particulier, G_0 est le sous-groupe d'inertie de G . Nous désignons par L_0 le corps d'inertie.

1.1 Groupes G_0 et G_1 .

Soit π une uniformisante de L . L'application qui, à $s \in G_0$, fait correspondre $s(\pi)/\pi$ définit par passage au quotient un isomorphisme θ_0 (indépendant du choix de π)

du groupe quotient G_0/G_1 sur un sous-groupe du groupe des racines de l'unité contenues dans le corps résiduel de L_0 . On en déduit que G_0 est produit semi-direct du p -groupe G_1 et d'un groupe cyclique C d'ordre premier à p ([5]). On pose, pour toute la suite :

$$\begin{aligned} r &= \text{card} (G_0/G_1) = \text{card} C, \\ p^n &= \text{card} (G_1), \end{aligned}$$

et on suppose $n \geq 1$ (i.e. l'extension L/K sauvagement ramifiée).

Idempotents e_χ .

Soit \mathfrak{X} le groupe multiplicatif des caractères de degré 1 de C , à valeurs dans L_0 . D'après ce qui précède, c'est un groupe d'ordre r , engendré par le caractère χ_0 qui induit par passage au quotient l'isomorphisme θ_0 . A chaque caractère $\chi \in \mathfrak{X}$ nous associons l'idempotent

$$e_\chi = \frac{1}{r} \sum_{s \in C} \chi(s^{-1})s$$

de l'algèbre $L_0[C]$. Les idempotents e_χ , $\chi \in \mathfrak{X}$, sont deux-à-deux orthogonaux et de somme 1. Tout $x \in L$ s'écrit donc de façon unique sous la forme $x = \sum_{\chi \in \mathfrak{X}} e_\chi(x)$, où chaque composante $e_\chi(x)$ est caractérisée par sa valuation :

PROPOSITION 1. — *Soit $\chi \in \mathfrak{X}$. Alors, pour tout $x \in L$, $x \neq 0$, on a $v(e_\chi x) \geq v(x)$, l'égalité ayant lieu si, et seulement si, $\chi = \chi_0^{v(x)}$.*

(On note v la valuation du corps L .)

La première assertion résulte du fait que les coefficients de e_χ sont entiers, la seconde est une conséquence immédiate de la définition de χ_0 à partir de l'isomorphisme θ_0 .

Opérations du groupe G/G_0 sur les groupes G_0/G_1 et \mathfrak{X} .

Le groupe G_0 étant produit semi-direct de G_1 par le groupe commutatif C , le quotient G/G_0 opère sur le quotient G_0/G_1 par automorphismes intérieurs. Par ailleurs, le quotient G/G_0 s'interprète comme le groupe de Galois de l'extension non ramifiée $L_0|K$, et opère donc sur le groupe \mathfrak{X} (par

composition). Plus précisément, le quotient G/G_0 s'identifie au groupe de Galois de l'extension résiduelle l_0/k , donc est engendré par la substitution de Frobenius de cette extension, qui opère sur \mathfrak{X} par $\chi \mapsto \chi^q$, avec :

$$q = \text{card}(k).$$

La proposition 1 permet de comparer les actions de G/G_0 sur les deux groupes cycliques (d'ordre r) G_0/G_1 et \mathfrak{X} :

COROLLAIRE. — *Ces opérations du groupe G/G_0 sur les groupes G_0/G_1 et \mathfrak{X} sont « les mêmes ».*

Explicitons : soit $g \in G$; il lui correspond un entier a modulo r tel que $gsg^{-1} \equiv s^a \pmod{G_1}$ pour tout $s \in G_0$. Montrons que l'on a $g\chi = \chi^a$ pour tout $\chi \in \mathfrak{X}$. Soit donc $\chi \in \mathfrak{X}$, et soit x un élément de L non nul et invariant par G_1 . On a :

$$e_{g\chi}(x) = ge_\chi g^{-1}(x), \quad \text{avec} \quad \chi' = \chi^a.$$

Comme le second membre a même valuation que $e_{\chi'}(x)$, on conclut $g\chi = \chi'$, par la proposition 1.

Exemples. — Supposons G abélien. L'opération de G/G_0 sur G_0/G_1 par automorphismes intérieurs est donc triviale. D'après le corollaire, il en va de même pour la permutation $\chi \rightarrow \chi^q$ de \mathfrak{X} . On en déduit que r divise $q - 1$.

Supposons G diédral. On voit facilement que les opérations de G/G_0 sont triviales sauf lorsque G_0 est le sous-groupe cyclique d'indice 2 de G . Dans ce cas, la substitution de Frobenius opère sur G_0/G_1 par : $\sigma \rightarrow \sigma^{-1}$. D'après le corollaire précédent, on a donc $\chi^{-1} = \chi^q$ pour tout $\chi \in \mathfrak{X}$, d'où l'on déduit que r divise $q + 1$.

1.2. Groupes supérieurs de ramification.

Soit t un nombre inférieur de ramification de l'extension L/K (c'est-à-dire un entier $t \geq 1$ tel que $G_t \neq G_{t+1}$). On sait que le quotient G_t/G_{t+1} est abélien de type (p, p, \dots, p) . Désignons par L_{G_t} le corps de ramification correspondant au groupe G_t . L'entier t est l'unique nombre de ramifi-

fication de l'extension $L_{G_{t+1}}/L_{G_t}$, et vérifie donc la majoration

$$t \leq \frac{p}{p-1} (G_0 : G_t) \quad (\text{cf. [1], corollaire à la prop. 4.2}).$$

Dans le cas où G_1 est cyclique, les quotients G_t/G_{t+1} sont d'ordre p , de sorte que la suite $(G_t)_{i \geq 1}$ des sous-groupes de ramification de G_1 est entièrement déterminée par les nombres inférieurs de ramification $0 < t_1 < t_2 < \dots < t_n$; nous allons voir que cette suite ne dépend que de l'écart entre t_1 et sa « valeur maximale » $\frac{rp}{p-1}$:

PROPOSITION 2. — *Supposons G_1 cyclique d'ordre p^n . Alors on a :*

1) $\frac{r}{p-1} \leq t_1 \leq \frac{rp}{p-1}$. De plus, si G_0 est cyclique, on a $t_1 = r$ sauf peut-être pour $p = 2$ auquel cas on peut aussi avoir $t_1 = 2r$.

2) pour $i = 2, \dots, n$:

$$t_i = \frac{rp^i}{p-1} - \left(\frac{rp}{p-1} - t_1 \right).$$

Démonstration. — 1) Le quotient G_0/G_1 opère sur G_t/G_{t+1} par automorphismes intérieurs. Soit g un générateur de G_0/G_1 , et soit $s \rightarrow s^a$ (avec $a \in (\mathbf{Z}/p\mathbf{Z})^*$) l'action de g sur le groupe G_t/G_{t+1} . Si l'on désigne par m l'ordre de a dans $(\mathbf{Z}/p\mathbf{Z})^*$, le p.p.c.m. de r et t_1 est mt_1 : en effet, on sait que $u \in G_0/G_1$ opère trivialement sur G_t/G_{t+1} si, et seulement si, $u^t = 1$ (cf. [5], chap. iv, § 3). Il en résulte que r divise $(p-1)t_1$ (et donc $t_1 \geq \frac{r}{p-1}$), et que, lorsque G_0 est commutatif, r divise t_1 . D'où l'on déduit 1) grâce à la majoration $t_1 \leq \frac{pr}{p-1}$.

2) Il suffit d'appliquer à la p -extension cyclique L/L_{G_t} les résultats de Fontaine ([1], prop. 4.3), compte tenu de la

minoration $t_1 \geq \frac{r}{p-1}$ (où r représente l'indice absolu de ramification de L_{G_1}).

Remarque. — Supposons $p \neq 2$, et G_0 diédral ou quaternionien. Alors G_1 est le sous-groupe cyclique d'indice 2, et l'on déduit de la démonstration de 1) que t_1 est impair ($r = 2$), la majoration $t_1 \leq \frac{2p}{p-1}$ conduit à $t_1 = 1$ sauf peut-être pour $p = 3$ auquel cas on peut aussi avoir $t_1 = 3$.

1.3. Ramification presque-maximale.

Nous associons à tout sous-groupe supérieur de ramification H de G l'idempotent $e_H = \frac{1}{\text{card } H} \sum_{s \in H} s$ de l'algèbre $K[G]$. Soit L_H le sous-corps de L fixe par H , B_H son anneau de valuation. L'ensemble $e_H B = \frac{1}{\text{card } H} \text{Tr}_{L/L_H}(B)$ est un idéal fractionnaire de L_H qui contient 1. On a donc $e_H B \supset B_H$, l'égalité ayant lieu si, et seulement si, e_H appartient à l'ordre \mathfrak{O} associé à B dans l'algèbre $K[G]$. Le résultat de Leopoldt laisse prévoir que, dans le cas d'une extension abélienne de \mathbf{Q}_p , tous les idempotents e_H appartiennent à \mathfrak{O} . Ce résultat n'est pas général :

Exemple. — Supposons $p \neq 2$, et soit L/K une extension abélienne totalement ramifiée de degré rp^2 (avec r premier à p), dont les sous-groupes supérieurs de ramification sont les suivants : $G_1 = \dots = G_t = H$ de type (p, p) $G_{t+1} = \{1\}$. [D'après la théorie du corps de classes local, une telle extension existe pourvu que K soit différent de \mathbf{Q}_p et contienne les racines r -ièmes de l'unité.] On a $t = r$ (G commutatif et $t \leq \frac{rp}{p-1}$). Soit \mathfrak{D} la différentielle de l'extension L/L_H . L'idéal fractionnaire $e_H B$ de B_H a pour valuation, dans L_H :

$$\nu_H(e_H B) = \left[\frac{1}{\text{card } H} \nu(\mathfrak{D}) \right] - \nu_H(\text{card } H),$$

(où pour tout réel x le symbole $[x]$ désigne le plus grand

entier $\leq x$). Or, on a $\nu(\mathcal{D}) = (r + 1)(\text{card } H - 1)$ (cf. [5], chap. IV, § 3), d'où :

$$\nu_{\mathbf{H}}(e_{\mathbf{H}}\mathbf{B}) = \left[\frac{1}{p^2} (r + 1)(p^2 - 1) \right] - 2r.$$

L'idempotent $e_{\mathbf{H}}$ n'appartient donc pas à \mathfrak{D} [et il suffit de choisir r assez grand ($r > p^2 - 1$) pour que $pe_{\mathbf{H}}$ n'appartienne pas non plus à \mathfrak{D}].

PROPOSITION 3. — *Supposons que tous les idempotents $e_{\mathbf{H}}$ appartiennent à \mathfrak{D} (lorsque \mathbf{H} décrit les sous-groupes supérieurs de ramification). Soit t un nombre inférieur de ramification. Alors on a :*

$$1) \quad \frac{p}{p-1} (G_0 : G_t) - 1 \leq t \leq \frac{p}{p-1} (G_0 : G_t);$$

2) *Le quotient G_t/G_{t+1} est cyclique d'ordre p sauf peut-être lorsque $p = 2$, auquel cas on peut aussi avoir G_2/G_3 de type (p, p) . Dans ce dernier cas, on a $G_0 = G_1 = G_2$.*

Démonstration. — Désignons ici par L_t le sous-corps de L fixe par G_t , par B_t l'anneau de valuation de L_t , et par ν_t la valuation dans L_t . L'hypothèse de la proposition 3 équivaut à $\text{Tr}_{L_t/L_t}(B) = \text{card}(G_t)B_t$ pour tout t , donc aussi à :

$$(1) \quad \text{Tr}_{L_{t+1}/L_t}(B_{t+1}) \subset (G_t : G_{t+1})B_t \text{ pour tout } t.$$

Fixons t , désignons par \mathcal{D} la différente de l'extension L_{t+1}/L_t , et posons $h = (G_t : G_{t+1}) = [L_{t+1} : L_t]$. La condition (1) s'explique ainsi :

$$\frac{1}{h} \nu_{t+1}(\mathcal{D}) \geq \nu_t(h),$$

soit encore :

$$\frac{1}{h} (t + 1)(h - 1) \geq \nu_t(h).$$

En rapprochant cette condition de la majoration

$$t \leq \frac{p}{p-1} \nu_t(p),$$

on obtient immédiatement les conditions 1) et 2) de la proposition 3. [En fait, ces conditions sont également suffisantes.]

Rappelons la définition suivante (cf. [2], § 6) :

On dit que la ramification de l'extension L/K est presque-maximale si, pour tout sous-groupe H compris entre deux groupes supérieurs de ramification consécutifs, l'idempotent e_H appartient à l'ordre \mathfrak{D} .

Nous voyons donc que, sauf dans le cas singulier ($p = 2$, $G_0 = G_1 = G_2$, G_2/G_3 de type (p,p)), l'hypothèse de la proposition 3 équivaut à « la ramification est presque-maximale » (grâce à la condition « K est absolument non ramifié »). On en déduit, par un résultat de Jacobinski, que sous l'hypothèse de la proposition 3 et en écartant le cas singulier, le groupe G_1 est cyclique sauf peut-être pour $p = 2$ auquel cas on peut aussi avoir la situation suivante : G_2 cyclique, $G_0 = G_1 = (s, G_2)$ avec $s^2 \in G_2$ (cf. [2], lemme 4). Réciproquement, nous obtenons le résultat suivant (à partir des propositions 2 et 3) :

COROLLAIRE. — *Supposons G_1 cyclique. Alors les conditions suivantes sont équivalentes :*

- (i) *la ramification est presque-maximale ;*
- (ii) *pour tout sous-groupe supérieur de ramification H , l'idempotent e_H appartient à \mathfrak{D} ;*
- (iii) *il existe un sous-groupe supérieur de ramification $H \neq \{1\}$ tel que e_H appartienne à \mathfrak{D} ;*
- (iv) *on a : $\frac{rP}{p-1} - t_1 \leq 1$.*

Exemples.

1) Supposons G_0 cyclique. Alors la ramification est presque-maximale si, et seulement si, l'une des deux conditions suivantes est vérifiée :

$$\left\{ \begin{array}{ll} t_1 = r & \text{et } r \leq p - 1 \\ \text{ou } t_1 = 2r & (\text{et } p = 2) . \end{array} \right.$$

2) Supposons G_0 diédral et $p \neq 2$. D'après la proposition 3, la ramification est presque-maximale si, et seulement si, $p = 3$ et $t_1 = 3$.

Cas d'une extension abélienne de \mathbb{Q} .

On sait que, dans ce cas, les groupes d'inertie sont cycliques sauf peut-être pour $p = 2$. Par ailleurs les entiers r divisent $p - 1$ (corollaire à la proposition 1). Nous retrouvons ainsi que, au moins pour les idéaux premiers ne divisant pas 2, la ramification d'une telle extension est presque-maximale.

2. ORDRES ASSOCIÉS A B

2.1. Généralités.

Nous associons à l'anneau de valuation B de L les ordres des algèbres $K[G]$, $L_0[G_0]$, $K[G_0]$ suivants :

$$\begin{aligned} \mathfrak{O}_{K[G]} &= \{\lambda \in K[G] / \lambda B \subset B\} \quad (\text{noté } \mathfrak{O} \text{ précédemment}), \\ \mathfrak{O}_{K[G_0]} &= \{\lambda \in K[G_0] / \lambda B \subset B\}, \\ \mathfrak{O}_{L_0[G_0]} &= \{\lambda \in L_0[G_0] / \lambda B \subset B\}. \end{aligned}$$

On a entre ces ordres les relations suivantes, qui permettent de se borner, pour la détermination explicite de $\mathfrak{O}_{K[G]}$, au cas d'une extension totalement ramifiée :

$$(2.1) \quad \mathfrak{O}_{K[G_0]} = \mathfrak{O}_{L_0[G_0]} \cap K[G_0],$$

et, par un théorème de Jacobinski ([2]) :

$$(2.2) \quad \mathfrak{O}_{K[G]} = \bigoplus_i \mathfrak{O}_{K[G_0]} s_i,$$

où $\{s_1, \dots, s_f\}$ est un système de représentants de G/G_0 . Par ailleurs, soit B_0 l'anneau de valuation du corps d'inertie L_0 . Nous verrons au paragraphe 3 que la structure de B comme module sur $\mathfrak{O}_{K[G_0]}$ (de rang f) est liée à la surjectivité de l'injection naturelle :

$$(2.3) \quad B_0 \otimes_A \mathfrak{O}_{K[G_0]} \hookrightarrow \mathfrak{O}_{L_0[G_0]}.$$

Pour étudier cette injection, il est commode de faire opérer le groupe G/G_0 sur l'algèbre $L_0[G_0]$ de la façon suivante : soit $\tau \in G/G_0$, $\lambda = \sum_{s \in G_0} a_s s \in L_0[G_0]$. On pose :

$$\tau \cdot \lambda = \sum_{s \in G_0} \tau(a_s) s.$$

PROPOSITION 4. — L'injection (2.3) est un isomorphisme si, et seulement si, l'ordre $\mathfrak{D}_{L_0[G_0]}$ est stable par l'opération « . » de G/G_0 .

Démonstration. — L'application (2.3) a pour image $B_0\mathfrak{D}_{K[G_0]}$, qui est stable par l'opération « . ». Si l'application est surjective, $\mathfrak{D}_{L_0[G_0]}$ sera donc stable également. Réciproquement, supposons $\mathfrak{D}_{L_0[G_0]}$ stable, et soit $\lambda \in \mathfrak{D}_{L_0[G_0]}$. Pour montrer que $\lambda \in B_0\mathfrak{D}_{K[G_0]}$, nous considérons un élément $x \in B_0$ tel que $B_0 = A[x]$. Alors, λ s'écrit de façon unique sous la forme :

$$\lambda = \sum_{0 \leq i \leq f-1} x^i \lambda_i, \quad \text{avec} \quad \lambda_i \in K[G_0],$$

et il s'agit de prouver que les λ_i appartiennent à $\mathfrak{D}_{L_0[G_0]}$ (donc à $\mathfrak{D}_{K[G_0]}$). Calculons-les : on a, pour tout

$$j = 0, 1, \dots, f-1 :$$

$$x^j \lambda = \sum_{0 \leq i \leq f-1} x^{i+j} \lambda_i,$$

d'où, en prenant les traces relatives à l'opération « . » :

$$\text{Tr}(x^j \lambda) = \sum_{0 \leq i \leq f-1} \text{Tr}_{L_0/K}(x^{i+j} \lambda_i).$$

Comme l'extension L_0/K est non ramifiée, la matrice $(\text{Tr}_{L_0/K}(x^{i+j}))_{i,j}$ est inversible. L'ordre $\mathfrak{D}_{L_0[G_0]}$ contient λ , donc $x^j \lambda$, donc aussi $\text{Tr}(x^j \lambda)$ (puisqu'il est stable), et donc les λ_i .

Désormais, nous supposons le groupe G_0 cyclique. Conformément aux notations générales, nous posons $\text{card } G_0 = rp^n$, r premier à p , $n \geq 1$; nous désignons par H_i le sous-groupe de G_0 d'ordre p^i ($0 \leq i \leq n$), et par C le sous-groupe de G_0 d'ordre r . Les sous-groupes supérieurs de ramification de G se répartissent sur $H_n, H_{n-1}, \dots, H_1, H_0 = \{1\}$. Enfin, nous notons plus simplement e_i les idempotents correspondants :

$$e_i = \frac{1}{p^i} \sum_{s \in H_i} s, \quad 0 \leq i \leq n.$$

Nous convenons de poser $e_{n+1} = 0$.

2.2 Cas d'une extension totalement ramifiée.

Nous faisons ici les hypothèses suivantes :

- { L'extension L/K est totalement ramifiée.
- { Le groupe G est cyclique.

Algèbre $K[G]$.

La décomposition de cette algèbre en produit direct d'algèbres simples repose sur les propriétés des extensions cyclotomiques de K suivantes, propriétés pour lesquelles l'hypothèse « K est absolument non ramifié » est essentielle :

LEMME 1. (cf. [5], chap. IV, § 4). — Soit ξ une racine primitive p^s -ième de l'unité, avec $s \geq 1$. Le corps $K(\xi)$ obtenu en adjoignant ξ à K est une extension totalement ramifiée de degré $(p-1)p^{s-1}$ de K . Son anneau de valuation est $A[\xi]$. L'élément $\xi - 1$ est une uniformisante de $K(\xi)$ et vérifie l'équation d'Eisenstein $F(1+X) = 0$, avec :

$$F(X) = X^{(p-1)p^{s-1}} + X^{(p-2)p^{s-1}} + \dots + 1.$$

Soit alors $\chi \in \mathfrak{X}$, et $i \in \{0, 1, \dots, n\}$. L'élément

$$e = e_\chi(e_i - e_{i+1})$$

de $K[G]$ est un idempotent primitif. Soit, en effet, ψ_i un caractère de degré 1 du groupe cyclique H_n , d'ordre p^{n-i} . L'idempotent e correspond au caractère irréductible de G dans K produit direct du caractère χ de C par le caractère $\varphi_i = \text{Tr}_{K(\psi_i)/K}(\psi_i)$ de H_n : en effet, l'irréductibilité du polynôme cyclotomique dans l'extension $K(\psi_i)/K$ implique, pour $i \neq 0$, $i \neq n$: $\varphi_i = \text{Ind}_{H_i}^{H_n}(\mathbf{1}_{H_i}) - \text{Ind}_{H_{i+1}}^{H_n}(\mathbf{1}_{H_{i+1}})$, (où $\mathbf{1}_H$ désigne le caractère trivial du groupe H). Pour $i = 0$ et $i = n$, on a des formules analogues.

Puisque tout caractère irréductible de G dans K est de la forme $\chi\varphi_i$, on voit que la famille

$$E = \{e_\chi(e_i - e_{i+1}), \chi \in \mathfrak{X}, 0 \leq i \leq n\}$$

constitue un système d'idempotents centraux primitifs de $K[G]$. Il lui correspond une décomposition de $K[G]$ en

corps cyclotomiques :

$$K[G] = \bigoplus_{e \in E} eK[G].$$

Soit \mathfrak{M} l'ordre maximal de $K[G]$ contenant $A[G]$. Il contient tous les idempotents e ; on a donc une décomposition

$$\mathfrak{M} = \bigoplus_{e \in E} e\mathfrak{M},$$

où la composante $e\mathfrak{M}$ est l'anneau de valuation du corps cyclotomique $eK[G]$. Précisons: pour $e = e_\chi(e_i - e_{i+1})$, $\chi \in \mathfrak{X}$, $0 \leq i \leq n$, $eK[G]$ est isomorphe au corps $K(\xi_i)$, où ξ_i est une racine primitive d'ordre p^{n-i} de 1; d'après le lemme 1, $e\mathfrak{M}$ est isomorphe à $A[\xi_i]$. En résultent les descriptions suivantes:

PROPOSITION 5. — *L'ordre maximal \mathfrak{M} est l'algèbre sur A engendrée par $A[G]$ et les idempotents e_i , $1 \leq i \leq n$.*

Et plus précisément :

LEMME 2. — *Posons $f = s - 1$, où s est un générateur de H_n . Soit $e = e_\chi(e_i - e_{i+1}) \in E$. On pose $m_i = [K(\xi_i) : K]$, ξ_i étant une racine primitive p^{n-i} ième de 1. Alors :*

1) *Les éléments ef^j , $0 \leq j \leq m_i - 1$, forment une base du A -module $e\mathfrak{M}$.*

2) *On a :*

$$(2.4) \quad \begin{cases} \text{pour } i = n : ef = 0. \\ \text{pour } i \neq n : ef^{m_i} = p(-1 + a_i f + \dots + l_i f^{m_i-1})e \\ \text{où } a_i, \dots, l_i \text{ sont des éléments de } A. \end{cases}$$

Ordre \mathfrak{D} associé à B dans l'algèbre $K[G]$.

D'après la proposition 5, \mathfrak{D} est contenu dans l'algèbre sur A engendrée par $A[G]$ et les e_i , l'égalité ayant lieu si, et seulement si, la ramification est presque-maximale. Remarquons que, sauf dans ce cas, \mathfrak{D} ne contient pas tous les idempotents primitifs, et n'est donc pas égal à la somme de ses composantes $e\mathfrak{D}$. Par contre, les idempotents e_χ appartiennent à $A[G]$, et l'on a donc

$$\mathfrak{D} = \bigoplus_{\chi \in \mathfrak{X}} e_\chi \mathfrak{D}.$$

Nous nous proposons de décrire la composante $e_\chi \mathfrak{D}$ pour un caractère χ fixé. Commençons par déterminer ceux des idempotents $e_\chi e_i$ qu'elle contient. Soit $i \in \{0, \dots, n\}$ un entier fixé. Posons $u_i = -\nu_i(e_i B)$ (où ν_i désigne la valuation dans $L_{\mathbb{H}_i}$), et $h_i = -\nu\left(\frac{1}{p^i} \mathfrak{D}_{L/L_{\mathbb{H}_i}}\right) + p^i - 1$. On a :

$$u_i = \left[\frac{1}{p^i} h_i \right], \quad \text{avec} \quad h_i = \left(\frac{rp}{p-1} - t_1 \right) (p^i - 1),$$

le nombre t_1 étant égal à r sauf peut-être pour $p = 2$, auquel cas on peut aussi avoir $t_1 = 2r$ (cf. proposition 2). Associons enfin au caractère χ et à l'entier i , l'entier $u_{i,\chi} \in \{1, 2, \dots, r\}$ défini par

$$\chi = \chi_0^{-p^i u_{i,\chi}},$$

et l'entier rationnel

$$h_{i,\chi} = h_i - p^i u_{i,\chi}.$$

LEMME 3. — 1) Soit $x \in B$. Alors on a $e_\chi e_i(x) \in B$ ou $\nu(e_\chi e_i(x)) = -p^i u_{i,\chi}$.

2) Soit $x \in L$. Alors :

si $\nu(x) > h_{i,\chi}$, on a $e_\chi e_i(x) \in B$;

si $\nu(x) = h_{i,\chi}$, on a $\nu(e_\chi e_i(x)) = -p^i u_{i,\chi}$.

3) On a les équivalences suivantes :

$$e_\chi e_i \in \mathfrak{D} \iff h_{i,\chi} < 0 \iff u_{i,\chi} > u_i.$$

Démonstration. — 1) Soit $x \neq 0$, $x \in B$. En appliquant la proposition 1, et les définitions de u_i et $u_{i,\chi}$, on obtient :

$$\nu_i(e_\chi e_i(x)) \equiv -u_{i,\chi} \pmod{r} \quad \text{et} \quad \nu_i(e_\chi e_i(x)) \geq -u_i > -r.$$

D'où l'on tire :

$$\nu_i(e_\chi e_i(x)) \in \{-u_{i,\chi}, r - u_{i,\chi}, 2r - u_{i,\chi}, \dots\}.$$

2) Soit $x \neq 0$, $x \in L$. On a :

$$\begin{aligned} \nu_i(e_i(xB)) &= \left[\frac{1}{p^i} \left(\nu(x) + \nu\left(\frac{1}{p^i} \mathfrak{D}_{L/L_{\mathbb{H}_i}}\right) \right) \right] \\ &= \left[\frac{1}{p^i} (\nu(x) - h_{i,\chi} + p^i - 1) \right] - u_{i,\chi}. \end{aligned}$$

On en déduit :

Si $\nu(x) > h_{i,\chi}$, on a : $\nu_i(e_i(x)) > -u_{i,\chi}$.

Si $\nu(x) = h_{i,\chi}$, on a : $\nu_i(e_i(x)) = -u_{i,\chi}$. En effet, $\nu_i(e_i(xB)) = u_{i,\chi}$, et il existe donc $y \in xB$ tel que $\nu_i(e_i(y)) = -u_{i,\chi}$.

D'après l'étude du cas précédent, on a $\nu(y) = \nu(x)$. L'extension L/K étant totalement ramifiée, il existe $a \in A^*$ tel que $x = ay$, d'où $\nu_i(e_i(x)) = -u_{i,\chi}$. On achève la démonstration de 2) (et donc de 3)), grâce à la proposition 1, et à 1).

L'ensemble I_χ des indices $i \in \{0, 1, \dots, n\}$ tels que l'idempotent $e_\chi e_i$ appartienne à \mathfrak{D} est donc donné par la formule :

$$I_\chi = \{i \in \{0, 1, \dots, n\} / u_{i,\chi} > u_i\}.$$

Nous allons voir que la connaissance des ensembles I_χ , $\chi \in \mathfrak{X}$, détermine celle de \mathfrak{D} . Introduisons la notation suivante : Pour tout sous-ensemble I de $\{0, 1, \dots, n\}$, pour tout $\chi \in \mathfrak{X}$, désignons par $\Lambda_\chi(I)$ le sous-A-module de $K[G]$ qui admet pour base les éléments suivants :

$$\begin{aligned} e_\chi e_i, \quad i \in I; \quad pe_\chi e_i, \quad i \in \complement I; \\ e_\chi e_i f^{j_i}, \quad 0 \leq i \leq n, \quad 1 \leq j_i \leq m_i - 1. \end{aligned}$$

($\complement I$ désigne le complémentaire de I dans $\{0, 1, \dots, n\}$, et les éléments f et m_i sont ceux du lemme 2.)

THÉORÈME 1. — Soit $\chi \in \mathfrak{X}$. On a $e_\chi \mathfrak{D} = \Lambda_\chi(I_\chi)$.

Il en résulte que l'ordre \mathfrak{D} est l'algèbre sur A engendrée par $A[G]$, les éléments $e_i f$ ($1 \leq i \leq n$), et les idempotents $e_\chi e_i$ tels que $i \in I_\chi$.

Démonstration du théorème 1. — Pour vérifier l'inclusion $\Lambda_\chi(I_\chi) \subset e_\chi \mathfrak{D}$, il suffit de prouver que les $e_i f$ appartiennent à \mathfrak{D} . Soient donc $i \in \{1, \dots, n\}$ et $x \in B$. Puisque $s \in G_{t_i}$, on a, dans le corps L_{H_i} :

$$\nu_i((s-1)e_i(x)) \geq t_1 + \nu_i(e_i(x)) \geq t_1 - u_i \geq r - u_i > 0.$$

Ainsi, $e_i f(x)$ appartient à B . Montrons maintenant l'inclusion $e_\chi \mathfrak{D} \subset \Lambda_\chi(I_\chi)$: Soit $\lambda \in e_\chi \mathfrak{D}$. Cet élément appartient à \mathfrak{M} et s'écrit donc sous la forme $\lambda = \alpha + \sum_{i \in I} a_i e_\chi e_i$, avec

$\alpha \in \Lambda_\chi(I_\chi)$, $I \subset \bigcup I_\chi$, et $a_i \in A^*$ (cela résulte de la définition de $\Lambda_\chi(I_\chi)$ et du lemme 2). Il s'agit de prouver que $I = \emptyset$, ce que nous déduisons du résultat suivant :

LEMME 4. — Soit I un ensemble non vide d'entiers $i \in \{0, 1, \dots, n\}$ tels que $e_\chi e_i \notin \mathfrak{D}$, et soit $\lambda = \sum_{i \in I} a_i e_\chi e_i$, avec $a_i \in A^*$ pour tout $i \in I$. Alors il existe $x \in B$ tel que $\nu(\lambda x) = \inf_{i \in I} (-p^i u_{i,\chi})$. En particulier, λ n'appartient pas à \mathfrak{D} .

Démonstration du lemme 4. — Par groupement dans λ des termes ayant même valeur de $-p^i u_{i,\chi}$, nous sommes ramenés au cas où $-p^i u_{i,\chi}$ est constant sur I . Soit a cette constante. La suite $h_{i,\chi}$ est strictement croissante sur I : en effet, on a $h_{i,\chi} = h_i - a = \frac{r}{p-1} (p^i - 1) - a$, puisque $t_1 = r$ (sinon la ramification serait presque-maximale, et I serait vide). Notons j le plus grand entier $\in I$, et soit $x \in L$ tel que $\nu(x) = h_{j,\chi}$. Appliquons le lemme 3: on a $x \in B$ (car $e_\chi e_j \notin \mathfrak{D}$), $\nu(e_\chi e_j(x)) = a$, et, pour $i \neq j$ ($i \in I$), $e_\chi e_i(x) \in B$. D'où l'on déduit $\nu(\lambda(x)) = a$. Ceci achève la démonstration du théorème 1.

2.3. Extension non totalement ramifiée.

Les formules (2.1) et (2.2) ramènent cette étude au cas précédent. Pour décrire explicitement les ordres $\mathfrak{D}_{L_0[G_0]}$, $\mathfrak{D}_{K[G_0]}$, et $\mathfrak{D}_{K[G]}$, introduisons les notations suivantes :

Soit $\chi \in \mathfrak{X}$, et soit $I \subset \{0, 1, \dots, n\}$. On note encore $\Lambda_\chi(I)$ la sous B_0 -algèbre de $L_0[G_0]$ définie comme dans le cas totalement ramifié, de sorte que, d'après le théorème 1, on a :

$$e_\chi \mathfrak{D}_{L_0[G_0]} = \Lambda_\chi(I_\chi).$$

Soit Γ un système de représentants des orbites de G/G_0 dans \mathfrak{X} . Pour tout $\chi \in \Gamma$, on pose :

$$\varepsilon_\chi = \sum_{\tau \in \text{Gal}(K(\chi)/K)} e_{\tau\chi} = \text{Tr}_\chi(e_\chi),$$

(où, pour tout $\lambda \in L_0[G_0]$, le symbole $\text{Tr}_\chi(\lambda)$ désigne

$\sum_{\tau \in \text{Gal}(\mathbb{K}(\chi)/\mathbb{K})} \tau \cdot \lambda)$. On pose enfin, pour tout $\chi \in \Gamma$:

$$\mathcal{J}_\chi = \bigcap_{\tau \in \text{Gal}(\mathbb{K}(\chi)/\mathbb{K})} I_{\tau\chi}.$$

Il est aisé de voir que \mathcal{J}_χ représente l'ensemble des entiers i tels que $\varepsilon_\chi e_i \in \mathfrak{D}_{\mathbb{K}[G_0]}$.

La connaissance des ensembles \mathcal{J}_χ détermine celle de $\mathfrak{D}_{\mathbb{K}[G_0]}$ et $\mathfrak{D}_{\mathbb{K}[G]}$:

COROLLAIRE 1. — Soit $\chi \in \Gamma$. On a :

$$\varepsilon_\chi \mathfrak{D}_{\mathbb{K}[G_0]} = \text{Tr}_\chi(\Lambda_\chi(\mathcal{J}_\chi)).$$

Démonstration. — L'inclusion $\text{Tr}_\chi(\Lambda_\chi(\mathcal{J}_\chi)) \subset \varepsilon_\chi \mathfrak{D}_{\mathbb{K}[G_0]}$ résulte immédiatement de l'inclusion $\mathcal{J}_\chi \subset I_\chi$ et du théorème 1. Montrons l'inclusion inverse. Soit donc $\lambda \in \mathfrak{D}_{\mathbb{K}[G_0]}$ et posons, pour tout $\varphi \in \mathfrak{X}$, $\lambda_\varphi = e_\varphi \lambda$. Puisque λ est invariant par l'opération « . », on a $\varepsilon_\chi \lambda = \text{Tr}_\chi(\lambda_\chi)$. Il nous reste donc à montrer que $\lambda_\chi \in \Lambda_\chi(\mathcal{J}_\chi)$. Soit $\tau \in \text{Gal}(\mathbb{K}(\chi)/\mathbb{K})$. Puisque $\lambda \in \mathfrak{D}_{\mathbb{K}[G_0]}$, on a $\lambda_{\tau\chi} \in \Lambda_{\tau\chi}(I_{\tau\chi})$. Or, puisque λ est invariant par l'opération « . », on a : $\tau^{-1} \cdot \lambda_{\tau\chi} = \lambda_\chi$. D'où l'on tire :

$$\lambda_\chi \in \tau^{-1} \cdot (\Lambda_{\tau\chi}(I_{\tau\chi})) = \Lambda_\chi(I_{\tau\chi}).$$

Ceci étant vrai pour tout τ , on voit que λ_χ appartient à $\Lambda_\chi(\mathcal{J}_\chi)$, d'où le résultat.

Du corollaire 1 on tire immédiatement :

COROLLAIRE 2. — L'ordre $\mathfrak{D}_{\mathbb{K}[G]}$ est l'algèbre sur A engendré par $A[G]$, les éléments $e_i f$ ($1 \leq i \leq n$), et les idempotents $\varepsilon_\chi e_i$ pour les couples (i, χ) tels que $i \in \mathcal{J}_\chi$.

COROLLAIRE 3. — L'ordre $\mathfrak{D}_{\mathbb{K}[G]}$ est contenu dans l'algèbre sur A engendré par $A[G]$ et les idempotents e_i , l'égalité ayant lieu si, et seulement si, la ramification est presque-maximale.

Remarques. — 1) Lorsque G_0 est cyclique, l'ordre $\mathfrak{D}_{\mathbb{K}[G]}$ contient les éléments pe_i et $e_i e_i$, pour tout i (1 désigne le caractère trivial). L'exemple du paragraphe 1 prouve que ce résultat n'est pas général.

2) Lorsque $K = \mathbf{Q}_p$, on peut montrer que \mathcal{I}_χ est égal à $\{0\}$ ou à $\{0, 1, \dots, n\}$. Bornons-nous à le vérifier dans le cas où G est diédral, G_0 cyclique, et $p \neq 2$. Nous savons qu'alors r divise $p + 1$. Deux cas peuvent donc se présenter :

Si $r \leq p - 1$, la ramification est presque-maximale. Les ordres $\mathfrak{D}_{K[G_0]}$, $\mathfrak{D}_{L_0[G_0]}$ et $\mathfrak{D}_{K[G]}$ admettent une description analogue à celle du théorème de Leopoldt.

Par contre, si $r = p + 1$, on a $u_i = 1$ pour tout $i \neq 0$. Les ensembles I_χ sont maximaux sauf pour $\chi = \chi_0$ ($I_\chi = \{0, 2, 4, \dots\}$) et $\chi = \chi_0^{-1}$ ($I_\chi = \{0, 1, 3, \dots\}$). Donc $\mathcal{I}_\chi = \{0, 1, 2, \dots, n\}$ sauf pour $\chi = \chi_0$ (et $\chi = \chi_0^{-1}$) auquel cas $\mathcal{I}_\chi = \{0\}$.

Étudions enfin la stabilité de l'ordre $\mathfrak{D}_{L_0[G_0]}$ par l'opération « . » de G/G_0 . Remarquons que l'on a, pour tout $\tau \in G/G_0$, $\tau \cdot (\Lambda_\chi(I_\chi)) = \Lambda_{\tau\chi}(I_\chi)$. L'ordre $\mathfrak{D}_{L_0[G_0]}$ est donc stable si, et seulement si, les ensembles I_χ sont constants sur chaque orbite. [Dans l'exemple précédent avec $r = p + 1$, cette condition n'est pas vérifiée pour $\chi = \chi_0$.] On obtient ainsi le critère suivant :

COROLLAIRE 4. — *Les conditions suivantes sont équivalentes :*

- (i) *L'ordre $\mathfrak{D}_{L_0[G_0]}$ est stable par l'opération « . »;*
- (ii) *Le groupe G/G_0 opère trivialement sur \mathfrak{X} ou bien la ramification est presque-maximale.*

Démonstration. — Compte tenu de l'équivalence

- (i) \iff « I_χ est constant sur chaque orbite », l'implication
- (ii) \implies (i) est évidente. Pour montrer la réciproque, nous utilisons un résultat plus précis :

LEMME 5. — *On suppose que le groupe G/G_0 n'opère pas trivialement sur \mathfrak{X} . Soit $i \in \{1, 2, \dots, n\}$. On désigne par \mathfrak{X}_i l'ensemble des caractères $\chi \in \mathfrak{X}$ tels que $e_\chi e_i$ n'appartienne pas à $\mathfrak{D}_{L_0[G_0]}$ (d'où $\mathfrak{X}_i = \{\chi \in \mathfrak{X} / u_{i,\chi} \leq u_i\}$). Les conditions suivantes sont équivalentes :*

- a) \mathfrak{X}_i est stable par G/G_0 ;
- b) on a $u_i = 0$ (i.e. $\mathfrak{X}_i = \emptyset$) ou $u_i \geq r - 1$ (i.e. $\mathfrak{X}_i = \mathfrak{X}$ ou $\mathfrak{X} - \{1\}$).

Démonstration du lemme 5. — Il suffit de montrer que *a*) entraîne *b*). Supposons donc \mathfrak{X}_i stable et $u_i \neq 0$. La bijection $\chi \rightarrow u_{i,\chi}$ de \mathfrak{X} sur $E = \{1, \dots, r\}$ applique \mathfrak{X}_i sur $E_i = \{1, \dots, u_i\}$. Par ailleurs l'action $\chi \rightarrow \chi^g$ du Frobenius de L_0/K se traduit, dans E , par la permutation g qui, à $u \in E$, associe l'élément $g(u)$ de E congru à qu modulo r . Remarquons que, puisque G/G_0 n'opère pas trivialement sur \mathfrak{X} , on a $g(1) \neq 1$. Par ailleurs, la stabilité de \mathfrak{X}_i se traduit par $g(E_i) = E_i$. Pour montrer $u_i \geq r - 1$, c'est-à-dire $r - 1 \in E_i$, il nous suffit donc de prouver que $g(r - 1) \in E_i$. Posons $u = g^{-1}(1)$. On a $u \neq 1$ et $u - 1 \neq u$ donc $u - 1$ et $g(u - 1) - 1$ appartiennent à E , d'où $g(r - 1) = g(u - 1) - 1$. Puisque l'ensemble E_i contient 1 ($u_i \neq 0$) et est stable par g , il contient les éléments $u, u - 1, g(u - 1), g(u - 1) - 1$, et $g(r - 1)$. C.Q.F.D.

Nous sommes maintenant en mesure d'achever la démonstration de l'implication (i) \implies (ii) du corollaire 4 : La condition (i) équivaut en effet à « \mathfrak{X}_i est stable pour tout $i = 1, 2, \dots, n$ ». Or l'expression de u_1 montre que la condition *b*) du lemme est, pour $i = 1$, équivalente à $u_1 = 0$. Ainsi, la stabilité de \mathfrak{X}_1 par G/G_0 équivaut à la condition (ii) du corollaire 4.

Remarque. — On sait que la stabilité de $\mathfrak{D}_{L_0[G_0]}$ est liée à la surjectivité de l'injection $B_0 \otimes \mathfrak{D}_{K[G_0]} \hookrightarrow \mathfrak{D}_{L_0[G_0]}$. Le corollaire 1 nous montre que, dans le cas général, l'image de $B_0 \otimes \mathfrak{D}_{K[G_0]}$ est $\bigoplus_{\chi \in \Gamma} \left(\bigoplus_{\varphi \in \text{orb } \chi} \Lambda_{\varphi}(\mathcal{J}_{\chi}) \right)$.

COROLLAIRE 5. — *On suppose $K = \mathbf{Q}_p$. Alors l'ordre $\mathfrak{D}_{L_0[G_0]}$ est stable par l'opération « . » si, et seulement si, la ramification est presque-maximale.*

Démonstration. — C'est immédiat.

Nous allons voir que la stabilité de $\mathfrak{D}_{L_0[G_0]}$ est nécessaire pour que B soit un module libre sur l'ordre $\mathfrak{D}_{K[G]}$.

3. STRUCTURES DE B SUR L'ORDRE DE $\mathfrak{D}_{K[G_0]}$

L'anneau B est un module de rang 1 sur $\mathfrak{D}_{K[G]}$ et de rang $f = [L_0 : K]$ sur $\mathfrak{D}_{K[G_0]}$, et la relation (2.2) entre

ces deux ordres montre que si B admet la base $\{x\}$ sur $\mathfrak{D}_{\mathbf{K}[G]}$, il admet la base $\{s_1(x), s_2(x), \dots, s_f(x)\}$ sur $\mathfrak{D}_{\mathbf{K}[G_0]}$ (où s_1, \dots, s_f est un système de représentants de G modulo G_0). Nous allons dans ce paragraphe donner deux types de conditions nécessaires pour que B soit libre sur $\mathfrak{D}_{\mathbf{K}[G_0]}$.

3.1. Relation avec la stabilité de $\mathfrak{D}_{L_0[G_0]}$.

THÉORÈME 2. — *Supposons que B soit un module libre sur $\mathfrak{D}_{\mathbf{K}[G_0]}$. Alors l'ordre $\mathfrak{D}_{L_0[G_0]}$ est stable par l'opération « . » de G/G_0 .*

Démonstration. — Montrons d'abord un résultat plus faible, valable sans hypothèse restrictive sur G_0 :

LEMME 6. — *Sous l'hypothèse du théorème 2, soient $\chi \in \mathfrak{X}$ tel que $e_\chi e_n \in \mathfrak{D}_{L_0[G_0]}$, et $\tau \in G/G_0$. Alors $e_{\tau\chi} e_n \in \mathfrak{D}_{L_0[G_0]}$.*

Démonstration. — Soit $\{x_1, \dots, x_f\}$ une base de B sur $\mathfrak{D}_{\mathbf{K}[G_0]}$, et soit $x \in B$. L'élément $e_\chi e_n(x)$ est entier (puisque $e_\chi e_n \in \mathfrak{D}_{L_0[G_0]}$), et s'écrit donc de façon unique:

$$(1) \quad e_\chi e_n(x) = \sum_j \lambda_j(x_j), \quad \text{avec} \quad \lambda_j \in \mathfrak{D}_{\mathbf{K}[G_0]}.$$

Précisons, pour un indice j fixé, la forme de λ_j : on a $\lambda_j = \varepsilon_\chi e_n \lambda_j = \text{Tr}(e_\chi e_n \lambda_j)$, où l'élément $e_\chi e_n \lambda_j$ est de la forme $b_j e_\chi e_n$, avec $b_j \in L_0$ (on a en effet $e_\chi e_n \mathbf{K}[G_0] = \mathbf{K}(\chi) e_\chi e_n$). Puisque l'ordre $\mathfrak{D}_{L_0[G_0]}$ contient $\text{Tr}_\chi(b_j e_\chi e_n)$, il contient en particulier $\tau.(b_j e_\chi e_n)$, c'est-à-dire $\tau(b_j) e_{\tau\chi} e_n$. Or, si on choisit $x \in B$ tel que $e_\chi e_n(x)$ n'appartienne pas à pB , il existe j tel que $b_j \notin pB_0$ (on déduit en effet de (1) $e_\chi e_n(x) = \sum b_j e_\chi e_n(x_j)$, avec $e_\chi e_n(x_j) \in B$). D'où l'on déduit $e_{\tau\chi} e_n \in \mathfrak{D}_{L_0[G_0]}$.

Ainsi, sous l'hypothèse du théorème 2, l'ensemble \mathfrak{X}_n défini par le lemme 5 est stable par G/G_0 . Si G/G_0 n'opère pas trivialement sur \mathfrak{X} , on a donc $u_n = 0$ ou $u_n \geq r - 1$. [Remarquons que ce résultat est valable sans hypothèse sur G_0 , si l'on pose $u_n = -\nu_H(e_H B)$ pour $H = G_1$.] Pour achever la démonstration du théorème 2, il reste à écarter l'éventualité $u_n \neq 0$, $u_n \geq r - 1$. Supposons donc $u_n \geq r - 1$,

et soit m le plus grand entier compris entre 1 et n tel que $u_m < r - 1$. On a donc $\mathfrak{X}_i = \mathfrak{X} - \{1\}$ pour $i \geq m + 1$, et \mathfrak{X}_m n'est pas stable par G/G_0 (lemme 5). Il existe donc $\chi \in \mathfrak{X}$ tel que $e_\chi e_m \in \mathfrak{D}_{L_0[G_0]}$ et $m \notin \mathcal{I}_\chi$. Nous allons en déduire $e_\chi e_n \in \mathfrak{D}_{L_0[G_0]}$, ce qui est absurde puisque $\chi \neq 1$. Soit donc $x \in B$. L'élément $e_\chi e_m(x)$ de B s'écrit sur la base $\{x_1, \dots, x_f\}$:

$$(1) \quad e_\chi e_m(x) = \sum_j \lambda_j(x_j), \quad \text{avec} \quad \lambda_j \in \mathfrak{D}_{K[G_0]}.$$

L'unicité de l'écriture (1) prouve que l'on a $\lambda_j = \varepsilon_\chi e_m \lambda_j$ pour tout j . Or, on déduit de (1) : $e_\chi e_n(x) = \sum_j e_\chi e_n \lambda_j(x_j)$. Il nous suffit donc de prouver que, pour tout $\lambda \in \mathfrak{D}_{K[G_0]}$ tel que $\lambda = \varepsilon_\chi e_m \lambda$, on a $e_\chi e_n \lambda \in \mathfrak{D}_{L_0[G_0]}$. En utilisant la définition de $\Lambda_\chi(\mathcal{I}_\chi)$ et le fait qu'aucun des entiers $m, m + 1, \dots, n$ n'appartient à \mathcal{I}_χ , on montre qu'un tel λ est de la forme $\lambda = \text{Tr}_\chi \left(\sum_{i \geq m} p b_i e_\chi e_i \right) + f \alpha$, avec $b_i \in B_0$, $\alpha \in \mathfrak{D}_{K[G_0]}$, $f = s - 1$ (s générateur de G_1). Il en résulte :

$$e_\chi e_n \lambda = \left(\sum_{i \geq m} p b_i \right) e_\chi e_n, \quad \text{d'où} \quad e_\chi e_n \lambda \in \mathfrak{D}_{L_0[G_0]}.$$

Ceci achève la démonstration du théorème 2.

Ce théorème admet une réciproque dans le cas particulier suivant :

COROLLAIRE. — *On suppose $K = \mathbf{Q}_p$. Alors B est un module libre sur $\mathfrak{D}_{K[G_0]}$ si, et seulement si, la ramification est presque-maximale.*

Démonstration. — Immédiate à partir du corollaire 5 au théorème 1, car dans ce cas la stabilité de $\mathfrak{D}_{L_0[G_0]}$ entraîne que l'ordre $\mathfrak{D}_{K[G_0]}$ est maximal.

Application.

Nous sommes maintenant en mesure de construire une extension sauvagement ramifiée de \mathbf{Q} dont l'anneau d'entiers n'est pas localement libre sur son ordre associé $\mathfrak{D}_{\mathbf{Q}[G]}$. Soient deux nombres premiers p et r tels que $p < r$ et que p engendre le groupe $(\mathbf{Z}/r\mathbf{Z})^*$. L'extension $N_1 = \mathbf{Q}(\sqrt[r]{1}, \sqrt[r]{p})$ est galoisienne (non abélienne!), modérément ramifiée en p .

L'hypothèse « p engendre le groupe $(\mathbf{Z}/r\mathbf{Z})^*$ » signifie que le premier p ne se décompose pas dans l'extension N_1/\mathbf{Q} . Soit N_2 une extension cyclique de \mathbf{Q} , de degré p^n , totalement ramifiée en p , et soit L le corps composé des extensions N_1 et N_2 de \mathbf{Q} . Comme la ramification en p n'est pas presque-maximale, l'anneau d'entiers de L n'est pas localement libre en p . Remarquons que toutes les extensions intermédiaires L'/\mathbf{Q} sauvagement ramifiées possèdent la même propriété.

Dans le cas général, la stabilité de $\mathfrak{D}_{L[\mathbf{G}_0]}$ n'implique pas une « grande » ramification, et la réciproque du théorème 2 n'est pas vraie.

3.2. Relation avec la ramification.

Supposons ici que le groupe G/G_0 opère trivialement sur \mathfrak{X} (par exemple G abélien), et soit $\chi \in \mathfrak{X}$. Avec les notations du corollaire 1 au théorème 1, on a $\varepsilon_\chi = e_\chi$, et la composante $e_\chi B$ est un module de rang $(G : G_0)$ sur l'anneau $e_\chi \mathfrak{D}_{K[\mathbf{G}_0]}$. Étudions cette structure :

PROPOSITION 6. — *Supposons que $e_\chi B$ soit un module libre sur $e_\chi \mathfrak{D}_{K[\mathbf{G}_0]}$. Alors, on a $pu_{i+1,\chi} > u_i$ pour tout i compris entre 0 et $n - 1$.*

Démonstration. — Soit i un entier fixé ($0 \leq i \leq n - 1$), et supposons $pu_{i+1,\chi} \leq u_i$. On voit facilement, en utilisant les définitions de $u_{i,\chi}$ et de I_χ , que cette condition équivaut à :

$$(i \notin I_\chi, \quad i + 1 \notin I_\chi, \quad \text{et} \quad pu_{i+1,\chi} = u_{i,\chi}).$$

Soit alors $\{x_1, x_2, \dots, x_f\}$ une base de $e_\chi B$ sur $e_\chi \mathfrak{D}_{K[\mathbf{G}_0]}$, et posons $y = e_\chi e_i(x_1)$, $z = e_\chi e_{i+1}(x_1)$. D'après ce qui précède, ces éléments de L_{H_i} ne sont pas entiers, et on a donc :

$$v_i(y) = -u_{i,\chi}, \quad v_i(z) = p(-u_{i+1,\chi}), \quad \text{d'où} \quad v_i(y) = v_i(z)$$

(lemme 3). Il existe donc $b \in B_0$ tel que $v_i(y - bz) > -u_{i,\chi}$, c'est-à-dire $y - bz \in B$ (lemme 3). La composante sur x_1 , dans l'écriture de $y - bz$ sur $\{x_1, x_2, \dots, x_f\}$ avec coefficients dans $K[\mathbf{G}_0]$, appartient donc à $\mathfrak{D}_{K[\mathbf{G}_0]}$. Or elle est de la

forme $e_\chi e_i + \sum_{j \geq i+1} a_j e_\chi e_j + \lambda$, avec $a_j \in A$ et $\lambda \in \mathfrak{D}_{K[G_0]}$.

D'après le lemme 4, ceci est en contradiction avec « $i \notin I_\chi$ ».

Or, pour que B soit un module libre sur $\mathfrak{D}_{K[G_0]}$, il faut et il suffit que chaque composante $e_\chi B$ soit libre sur $e_\chi \mathfrak{D}_{K[G_0]}$. Nous obtenons ainsi la condition « $u_{n-1} \leq p$ » nécessaire pour que B soit libre sur $\mathfrak{D}_{K[G_0]}$. Cette condition signifie, pour $n > 1$, que la ramification est « suffisamment » forte, puisqu'on peut l'expliciter ainsi :

$$\frac{rp}{p-1} - t_1 \leq p \frac{p^{n-1}}{p^{n-1}-1},$$

à condition d'attribuer au deuxième membre la valeur $+\infty$ pour $n = 1$.

Remarque. — Nous voyons que, pour $K \neq \mathbf{Q}$, les conditions « r divise $q-1$ » (i.e. G/G_0 opère trivialement sur

\mathfrak{K}) et $\frac{rp}{p-1} - t_1 > p$ sont compatibles; il existe donc des extensions abéliennes (et même cycliques) de K pour lesquelles B n'est pas libre sur $\mathfrak{D}_{K[G_0]}$ (et donc sur $\mathfrak{D}_{K[G]}$). Par contre, lorsque $K = \mathbf{Q}_p$, la condition « G abélien » implique que la ramification est presque-maximale, et donc que B est libre sur $\mathfrak{D}_{K[G_0]}$.

Nous allons montrer que, lorsque l'extension est totalement ramifiée, la proposition 6 admet une réciproque.

4. STRUCTURE DE B SUR $\mathfrak{D}_{K[G]}$ DANS LE CAS D'UNE EXTENSION TOTALEMENT RAMIFIÉE

Nos hypothèses sont ici :

- 1) L'extension L/K est totalement ramifiée.
- 2) Le groupe G est cyclique.

THÉORÈME 3. — *Soit $\chi \in \mathfrak{X}$. Les conditions suivantes sont équivalentes :*

- a) la composante $e_\chi B$ est un module libre sur $e_\chi \mathfrak{D}$.
- b) $pu_{i+1, \chi} > u_i$ pour tout $i \in \{0, 1, \dots, n-1\}$.

D'où l'on déduit :

COROLLAIRE. — *L'anneau B est un module libre sur l'ordre \mathfrak{D} si, et seulement si, l'on a :*

$$(1) \quad \frac{rp}{p-1} - t_1 < \frac{p^n}{p^{n-1} - 1}.$$

(Avec la convention usuelle pour $n = 1$.)

Explicitons la condition (1) :

$$\left\{ \begin{array}{l} \text{si } \frac{rp}{p-1} - t_1 \leq p \text{ (i.e. } t_1 = 2r \text{ ou } t_1 = r \text{ et } r < p(p-1)), \\ \quad (1) \text{ est toujours vraie} \\ \text{si } p < \frac{rp}{p-1} - t_1 \leq p+1 \text{ (i.e. } t_1 = r \text{ et } p(p-1) < r < p^2), \\ \quad \text{on a : } (1) \iff n \leq 2 \\ \text{si } p+1 < \frac{rp}{p-1} - t_1 \text{ (i.e. } t_1 = r \text{ et } r > p^2), \text{ on a} \\ \quad (1) \iff n \leq 1. \end{array} \right.$$

On remarque en particulier que si la propriété « B est libre sur \mathfrak{D} » est vraie pour l'extension L/K , elle est vraie pour toute extension L'/K intermédiaire.

Exemple. — Soit $K = \mathbf{Q}_p$, avec $p \neq 2$, et soit L/K une extension diédrale à groupe d'inertie cyclique, avec $r = p + 1$. On a alors $\frac{rp}{p-1} - t_1 = \frac{p+1}{p-1}$, de sorte que B est libre sur $\mathfrak{D}_{L_0[G_0]}$. Nous avons vu au paragraphe 3 qu'il n'est pas libre sur $\mathfrak{D}_{K[G_0]}$ ni sur $\mathfrak{D}_{K[G]}$.

La fin du paragraphe est consacrée à la démonstration, par récurrence sur n , de l'implication $b) \implies a)$. Pour $n = 0$, la condition $a)$ est vérifiée puisque la ramification est modérée. Supposons l'implication $b) \implies a)$ vraie au rang $n - 1$, et soit L/K une extension de degré rp^n vérifiant, pour le caractère χ fixé, la condition $b)$. Nous supposons de plus $t_1 = r$ (sinon, l'ordre \mathfrak{D} est maximal, et la condition $a)$ est vérifiée).

Notons ici L' le sous-corps fixe par le sous-groupe d'ordre p de G , et soient B' son anneau de valuation, G' le

groupe de Galois de l'extension L'/K , \mathfrak{D}' l'ordre associé à B' dans l'algèbre $K[G']$. Identifions le sous-groupe C de G avec son image dans G' . L'extension L'/K est de degré rp^{n-1} et vérifie la condition b) pour le caractère χ . En effet, soit $i \in \{0, \dots, n-1\}$, et soit $u'_{i,\chi}$ l'entier associé à i et χ pour l'extension L'/K . On a $u'_{i,\chi} = u_{i+1,\chi}$ (le caractère χ'_0 associé à L'/K est χ'_0), et $u'_i = u_i$ (le nombre t'_1 relatif à L'/K est égal à r). D'où :

$$pu'_{i+1,\chi} = pu'_{i+2,\chi} > u_{i+1} \geq u_i.$$

D'après l'hypothèse de récurrence, il existe $x' \in e_\chi B'$ tel que $e_\chi B' = e_\chi \mathfrak{D}' x'$. Nous allons construire, à partir de x' , une base $\{x\}$ de $e_\chi B$ sur $e_\chi \mathfrak{D}$.

I. — Étudions d'abord l'incidence de la condition b) sur les ensembles $I_\chi = \{i \in \{0, \dots, n\} / e_\chi e_i \in \mathfrak{D}\}$ et $I'_\chi = \{i \in \{0, \dots, n-1\} / e_\chi e'_i \in \mathfrak{D}'\}$, où e'_i désigne l'idempotent de $K[G']$ qui correspond au sous-groupe d'indice p^i .

LEMME 7. — Soit $j+1$ le premier entier ≥ 1 appartenant à I_χ ($j=0$ si $1 \in I_\chi$; $j=n$ si $I_\chi = \{0\}$), et soit $i \geq 1$. Alors :

- 1) si $i \leq j$, on a $u_{i,\chi} \not\equiv 0(p)$ et $h_{i,\chi} = h_{1,\chi}$;
 - 2) si $i \leq j$, alors $i-1 \in I'_\chi$;
- si $i > j$, alors on a l'équivalence : $i-1 \in I'_\chi \iff i \in I_\chi$.

Démonstration. — Il résulte des définitions de $u_{i,\chi}$ et $h_{i,\chi}$ (cf. § 2,2), que l'on a $pu_{i+1,\chi} = u_{i,\chi} + a_i r$, avec $a_i \in \{0, \dots, p-1\}$, et $h_{i+1,\chi} = h_{i,\chi} + rp^i(1 - a_i)$. On a les implications suivantes :

$$\left\{ \begin{array}{l} i+1 \notin I_\chi \implies pu_{i+1,\chi} \leq pu_{i+1} \implies pu_{i+1,\chi} \leq 2r \implies (a_i=0 \text{ ou } a_i=1). \\ (i \in I_\chi, i+1 \notin I_\chi) \implies h_{i+1,\chi} \neq h_{i,\chi} \implies a_i = 0. \\ i \notin I_\chi \implies a_i \neq 0 \text{ (condition } b)). \\ i \notin I_\chi, i+1 \notin I_\chi \implies a_i = 1. \end{array} \right.$$

Il en résulte, en particulier, $a_1 = a_2 = \dots = a_{j-1} = 1$ et $a_j \geq 1$, ce qui démontre 1). Remarquons que, réciproquement, si $a_1 = a_2 = \dots = a_{i-1} = 1$, alors on a $i \leq j$. Pour montrer 2), rappelons que

$$I'_\chi = \{i \in \{0, \dots, n-1\} / h'_{i,\chi} < 0\},$$

avec

$$h'_{i,\lambda} = h_i - p^i u'_{i,\lambda} = r((1 - a_1) + (1 - a_2)p + \dots + (1 - a_i)p^{i-1}) - u_{1,\lambda}.$$

D'où :

- a) si $i \leq j$, on a $h'_{i-1,\lambda} = -u_{1,\lambda} < 0$;
- b) si $i > j$, posons $m = (1 - a_1) + \dots + (1 - a_{i-1})p^{i-2}$.

On a alors :

$$\begin{aligned} h'_{i-1,\lambda} &= rm - u_{1,\lambda}, \\ \text{et } h_{i,\lambda} &= ph'_{i-1,\lambda} + r = (pm + 1)r - pu_{1,\lambda}. \end{aligned}$$

D'où les implications :

$$\begin{aligned} h'_{i-1,\lambda} > 0 &\implies h_{i,\lambda} > 0 \\ h_{i,\lambda} > 0 &\implies m \geq 0 \implies \begin{cases} m \geq 1 \\ \text{ou} \\ m = 0 \end{cases} \\ &\implies \begin{cases} h'_{i-1,\lambda} > 0 \\ \text{ou} \\ a_1 = 1, a_2 = 1, \dots, a_{i-1} = 1 \end{cases} \implies \begin{cases} h'_{i-1,\lambda} > 0 \\ \text{ou} \\ i \leq j \end{cases} \end{aligned}$$

ceci achève la démonstration de 2).

II. — D'après le théorème 1, le A-module $e_\lambda \mathfrak{D}$ admet pour base les p^n éléments suivants :

$$\begin{aligned} e_\lambda e_i, \quad i \in I_\lambda; \quad pe_\lambda e_i, \quad i \notin I_\lambda; \\ e_\lambda e_i f^{j_i}, \quad 0 \leq i \leq n, \quad 1 \leq j_i \leq m_i - 1. \end{aligned}$$

On désigne par \mathcal{B} cette base ordonnée suivant l'ordre lexicographique pour les couples (i, j_i) . Un élément x de $e_\lambda \mathfrak{B}$ est une base de $e_\lambda \mathfrak{B}$ sur $e_\lambda \mathfrak{D}$ si et seulement si les éléments $\lambda(x)$, $\lambda \in \mathcal{B}$, forment une base sur $e_\lambda \mathfrak{B}$ sur A , donc si, et seulement si, ces éléments sont linéairement indépendants modulo $p\mathfrak{B}$:

$$\sum_{\lambda \in \mathcal{B}} a_\lambda \lambda(x) \equiv 0(p\mathfrak{B}), \quad \text{avec } a_\lambda \in A,$$

$$\implies a_\lambda \equiv 0(pA) \quad \text{pour tout } \lambda \in \mathcal{B}.$$

Désignons par \mathcal{B}_0 la suite des éléments de \mathcal{B} correspondant à $i = 0$ ($\mathcal{B}_0 = \{e_\lambda e_0, e_\lambda e_0 f, \dots, e_\lambda e_0 f^{m_0-1}\}$), et par \mathcal{B}_1 le complémentaire dans \mathcal{B} .

1) Il existe $y \in e_\gamma B$ vérifiant la condition (1) :

$$(1) \quad \begin{cases} \text{si } j = 0 : (e_0 - e_1)f^{m_0-1}(y) \notin pB \\ \text{si } j \geq 1 : v(y) = h_{1,\gamma}, \end{cases}$$

(où j est l'entier défini dans le lemme 7).

L'existence de y résulte, dans le cas $j = 0$, du fait que $\frac{1}{p}(e_0 - e_1)f^{m_0-1}$ n'appartient pas à \mathfrak{D} , et dans le cas $j \geq 1$, des équivalences : $j \geq 1 \iff 1 \notin I_\gamma \iff h_{1,\gamma} \geq 0$. Montrons que pour un tel y , les éléments $\lambda(y)$, $\lambda \in \mathfrak{B}_0$, sont linéairement indépendants modulo $pB + B'$. Nous allons utiliser les formules 2.4 :

$$\begin{cases} e_n f = 0 \\ \text{pour } 0 \leq i < n : (e_i - e_{i+1})f^{m_i} \equiv -p(e_i - e_{i+1}) \pmod{pf\mathfrak{D}}. \end{cases}$$

Soit une congruence $\sum_{\lambda \in \mathfrak{B}_0} a_\lambda \lambda(y) \equiv 0 \pmod{pB + B'}$, avec $a_\lambda \in A$, et supposons qu'il existe un $a_\lambda \not\equiv 0 \pmod{pA}$. Par multiplication par une puissance convenable de f , on en déduit $f^{m_0-1}(y) \equiv 0 \pmod{pB + B'}$. Si $j = 0$, $e_0 - e_1$ appartient à \mathfrak{D} . On trouve donc $(e_0 - e_1)f^{m_0-1}(y) \equiv 0 \pmod{pB}$, ce qui est contraire au choix de y .

Supposons $j > 0$. Par application de f , on trouve $f^{m_0}(y) \equiv 0 \pmod{pf(B) + B'}$, il existe donc $z \in B$ tel que $y + f(z) \in L'$, donc tel que l'on ait :

$$v(y + f(z)) \equiv 0 \pmod{pZ}.$$

Or on a :

$$v(f(z)) \geq r + 1,$$

d'où :

$$v(y + f(z)) = v(y) = r - pu_{1,\gamma} \not\equiv 0 \pmod{pZ}.$$

Ainsi, pour tout $y \in e_\gamma B$ vérifiant (1), les éléments $\lambda(y)$, $\lambda \in \mathfrak{B}_0$, sont linéairement indépendants modulo $pB + B'$.

Soit $x \in e_\gamma B$ vérifiant la condition (1), et soit la congruence $\sum_{\lambda \in \mathfrak{B}} a_\lambda \lambda(x) \equiv 0 \pmod{pB}$. On en déduit (puisque, pour $\lambda \in \mathfrak{B}_1$, $\lambda(x)$ appartient à B') :

$$\sum_{\lambda \in \mathfrak{B}_0} a_\lambda \lambda(x) \equiv 0 \pmod{pB + B'},$$

d'où l'on tire: $a_\lambda \equiv 0(pA)$ pour tout $\lambda \in \mathcal{B}_0$, et donc $\sum_{\lambda \in \mathcal{B}_1} a_\lambda \lambda(x) \equiv 0(pB')$. On voit donc que, si les éléments $\lambda(x)$, $\lambda \in \mathcal{B}_1$, sont linéairement indépendants modulo pB' , alors $\{x\}$ est une base de $e_\lambda B$ sur $e_\lambda \mathfrak{D}$. Désignons par \mathcal{B}' la base de $e_\lambda \mathfrak{D}'$ sur A ordonnée dans l'ordre lexicographique des couples (i, j) . La matrice des éléments $\lambda(x)$, $\lambda \in \mathcal{B}_1$ dans la base $\lambda'(x')$, $\lambda' \in \mathcal{B}'$ de $e_\lambda B'$ sur A est de la forme :

$$\begin{bmatrix} M_1(x) & & & 0 \\ * & M_2(x) & & \\ & & \ddots & \\ * & * & & M_n(x) \end{bmatrix}$$

où $M_i(x)$ est, pour $i \in \{1, \dots, n\}$, une matrice carrée d'ordre m_i .

D'après ce qui précède, un élément x de $e_\lambda B$ vérifiant (1) est une base de $e_\lambda B$ sur $e_\lambda \mathfrak{D}$ si, et seulement, si chaque matrice $M_i(x)$ est inversible.

2) Soit $y \in e_\lambda B$ vérifiant la condition (1) et posons :

$$x = y - e_{j+1}(y) + e'_j(x') \quad (\text{lorsque } j = n, \quad x = y),$$

où l'entier j est défini par le lemme 7. Par définition, $j + 1 \in I_\lambda$, et donc $j \in I'_\lambda$ (lemme 7). L'élément x appartient donc à $e_\lambda B$. De plus, il est congru à y modulo B' , et vérifie donc la condition (1). Montrons que toutes les matrices $M_i(x)$ sont inversibles.

a) Supposons $i > j$. On a alors $e_i(x) = e'_{i-1}(x')$. Compte tenu de l'équivalence $i \in I_\lambda \iff i - 1 \in I'_\lambda$ (lemme 7), la matrice $M_i(x)$ est la matrice identité d'ordre m_i .

b) Supposons $i \leq j$, et posons $e = e_\lambda e_i$, $e' = e_\lambda e'_{i-1}$, $m = m_i (= m'_{i-1})$, et $C = B_{\mathbb{H}_{i+1}} + pB_{\mathbb{H}_i}$. En écrivant $ef(x)$ sur la base $\lambda'(x')$, $\lambda' \in \mathcal{B}'$, on obtient, puisque e' appartient à \mathfrak{D}' (lemme 7) :

$$\begin{cases} ef(x) & \equiv e'(a + bf + \dots + kf^{m-2} + lf^{m-1})(x') & (\text{mod. } C) \\ ef^2(x) & \equiv e'(af + \dots + kf^{m-1})(x') & (\text{mod. } C) \\ \dots & \\ ef^{m-1}(x) & \equiv e'(af^{m+2} + bf^{m-1})(x') & (\text{mod. } C) \\ -pe(x) & \equiv e'(af^{m-1})(x') & (\text{mod. } C) \end{cases}$$

(où a, b, \dots, k, l sont des éléments de A). La matrice $M_i(x)$ est donc, modulo p , de la forme :

$$M_i(x) = \begin{bmatrix} 0 & a & 0 & \dots & 0 \\ 0 & * & a & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & * & * & \dots & a \\ -a & * & * & \dots & * \end{bmatrix}$$

et il suffit donc de vérifier que l'on a : $a \not\equiv 0(pA)$, c'est-à-dire $e(x) \notin C$. Or, puisque x vérifie (1), on a

$$v(x) = h_{1,\lambda} = h_{2,\lambda} = \dots = h_{i,\lambda} \quad (\text{lemme 7});$$

l'élément $e(x)$ a donc pour valuation, dans L_{H_i} , $-u_{i,\lambda}$ (lemme 3), et $u_{i,\lambda}$ n'est pas divisible par p (lemme 7). La matrice $M_i(x)$ est donc inversible.

Finalement, nous avons construit une base $\{x\}$ de $e_\lambda B$ sur $e_\lambda \mathfrak{D}$. Ceci achève la démonstration du théorème 3.

BIBLIOGRAPHIE

- [1] J.-M. FONTAINE, *Ann. Scient. Sc. Norm. Sup* 4^e série, 4, n^o 3 (1971).
- [2] H. JACOBINSKI, Über die Hauptordnung eines Körpers als Gruppenmodul, *J. reine angew. Math.*, 213 (1963), 151-164.
- [3] H. W. LEOPOLDT, Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers, *J. reine angew. Math.*, 201 (1959), 119-149.
- [4] E. NOETHER, Normal basis bei Körpern ohn höhere Verzweigung, *Jour. reine angew. Math.*, 167 (1932), 147-152.
- [5] J.-P. SERRE, *Corps locaux*, 2^e éd., Hermann, Paris, 1968.

Manuscrit reçu le 12 décembre 1977

Proposé par J. Martinet.

Anne-Marie BERGÉ,
U.E.R. de Mathématiques
et d'Informatique de l'Université
de Bordeaux I
351, cours de la Libération
33405 Talence Cedex.