Journal de Théorie des Nombres
de Bordeaux **6** *(1994), 95–116*

Bases normales d'entiers dans les extensions de Kummer de degré premier

par E. J. Gómez Ayala

Abstract – If F is a number field, we denote by $\mathfrak{O}_F$ its ring of integers. Let E/F be a finite Galois extension of number fields with group G; a basis of $\mathfrak{O}_E$ as $\mathfrak{O}_F$-module of the form $\{a^g\}_{g\in G}$ is called a normal basis of $\mathfrak{O}_E$ over $\mathfrak{O}_F$. In this paper we establish an existence criterion for an integral normal basis in a Kummer extension of prime degree, which shows in addition how to construct a normal basis in case it exists. The main tools used in the proof are a formula of Fröhlich for the resolvents and a theorem of Hecke describing the ramification in a Kummer extension of prime degree. As an application, we show how to use our criterion to deduce a normal basis theorem obtained by F. Kawamoto.

Résumé – Si F est un corps de nombres, on note $\mathfrak{O}_F$ son anneau d'entiers; si E/F est une extension galoisienne finie de corps de nombres de groupe de Galois G, on appelle base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$ toute base de $\mathfrak{O}_E$ en tant que $\mathfrak{O}_F$-module de la forme $\{a^g\}_{g\in G}$ avec $a \in \mathfrak{O}_E$. On démontre dans ce travail un critère d'existence de base normale d'entiers pour les extensions de Kummer de degré premier, qui permet une construction explicite en cas d'existence; les principaux outils pour la démonstration sont une formule de Fröhlich pour les résolvantes ainsi qu'un critère de Hecke qui décrit la ramification dans une extension de Kummer de degré premier. Comme application, on utilise ce critère pour déduire un théorème de base normale obtenu par F. Kawamoto.

Si F est un corps de nombres, on note $\mathfrak{O}_F$ son anneau d'entiers. Soit E/F une extension galoisienne finie de corps de nombres de groupe de Galois G; on dit que $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$ s'il existe un élément a de $\mathfrak{O}_E$ tel que $\{a^g\}_{g\in G}$ constitue une base de $\mathfrak{O}_E$ en tant que $\mathfrak{O}_F$-module (autrement dit, s'il existe une base $\{a\}$ de $\mathfrak{O}_E$ en tant que $\mathfrak{O}_F[G]$-module). Plus généralement, si $\mathfrak{A}_E$ est l'ordre associé de $\mathfrak{O}_E$ dans $F[G]$ (c'est à dire, le plus grand ordre de $F[G]$ qui opère sur $\mathfrak{O}_E$), l'étude de la structure de $\mathfrak{O}_E$ comme $\mathfrak{A}_E$-module constitue ce qu'on appelle l'étude de la structure galoisienne relative de $\mathfrak{O}_E$; lorsque E/F est modérément ramifiée, $\mathfrak{A}_E = \mathfrak{O}_F[G]$ et dire que $\mathfrak{O}_E$ est libre comme $\mathfrak{A}_E$-module équivaut à dire qu'il existe une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.

Manuscrit reçu le 15 janvier 1993.

Plusieurs auteurs ont étudié la structure galoisienne relative de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$ lorsque E/F est une extension de Kummer modérément ramifiée ou non ([3], [13], [16]), mais à notre connaissance il n'existe aucun critère explicite d'existence de base normale d'entiers pour les extensions de Kummer modérément ramifiées.

Un tel critère constitue le résultat principal de ce travail. Plus précisément, soit l un nombre premier et soit E/F une extension de Kummer de degré l de groupe de Galois G. Supposons que $\mathfrak{a}$ est un idéal de $\mathfrak{O}_F$ qui possède une décomposition de la forme :

$$\mathfrak{a} = \prod_{i=1}^{l-1} \mathfrak{a}_i^i, \tag{1}$$

où les $\mathfrak{a}_i$ sont des idéaux de $\mathfrak{O}_F$ premiers entre eux et sans facteur carré. On définit les idéaux $\mathfrak{b}_j$ $(0 \leq j \leq l-1)$ associés à $\mathfrak{a}$ par :

$$\mathfrak{b}_j = \prod_{i=1}^{l-1} \mathfrak{a}_i^{[ij/l]}, \tag{2}$$

où $[x]$ est la partie entière de x, c'est à dire le plus grand entier inférieur ou égal à x. On remarque qu'on a toujours $\mathfrak{b}_0 = \mathfrak{b}_1 = \mathfrak{O}_F$.

Théorème 2.1. *Soit E/F une extension de Kummer modérément ramifiée de degré l premier. Alors $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$ si et seulement s'il existe $\alpha \in \mathfrak{O}_E$ avec $\alpha^l \in \mathfrak{O}_F$, $E = F(\alpha)$, et tel que $\alpha^l \mathfrak{O}_F$ admette une décomposition de la forme :*

$$\alpha^l \mathfrak{O}_F = \prod_{i=1}^{l-1} \mathfrak{a}_i^i,$$

où les $\mathfrak{a}_i$ sont des idéaux entiers de F, premiers entre eux et sans facteur carré, tels que les idéaux $\mathfrak{b}_j$ $(0 \leq j \leq l-1)$ sont principaux, avec des générateurs x_j tels que :

$$\sum_{j=0}^{l-1} (\alpha^j / x_j) \equiv 0 \mod l.$$

En outre dans ce cas $(1/l)\sum_{j=0}^{l-1}(\alpha^j/x_j)$ engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.

Dans le §1, on introduit les outils nécessaires à la démonstration du théorème 2.1, qui est démontré dans le §2. Dans le §3, on examine le cas particulier des extensions de Kummer non ramifiées et on développe d'un point de vue explicite un exemple récemment considéré par M. J. Taylor ([18], chap. IV). Enfin dans le §4 on montre comment on peut déduire du théorème 2.1 un théorème de base normale obtenu par F. Kawamoto.

Ce travail constitue essentiellement le troisième chapitre de la thèse de l'auteur à l'université Bordeaux I. Je veux exprimer ici ma reconnaissance à mon directeur de thèse Philippe Cassou-Noguès pour les nombreuses améliorations qu'il a apportées à la première version.

1. Préliminaires

Soit E/F une extension abélienne de corps de nombres et soit $G = \mathrm{Gal}(E/F)$. Soit $\hat{G}$ le groupe des caractères de G, c'est-à-dire le groupe des homomorphismes de G dans $\mathbf{C}^*$. Pour tout $a \in E$ et tout $\Phi \in \hat{G}$, on définit la résolvante de Lagrange $(a|\Phi)$ par :

$$(a|\Phi) = \sum_{g \in G} a^g \Phi(g^{-1}). \tag{3}$$

On va noter $D_{E/F}$ le discriminant de l'extension E/F.

Proposition 1.1. *Soit E/F une extension abélienne et modérément ramifiée de corps de nombres, $G = \mathrm{Gal}(E/F)$ et $a \in \mathfrak{O}_E$ tel que $E = aF[G]$. Alors $\{a^g\}_{g \in G}$ est une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$ si et seulement si :*

$$D_{E/F} = \Big(\prod_{\chi \in \hat{G}} (a|\chi)^2\Big)\,\mathfrak{O}_F.$$

Si $\{a^g\}_{g \in G}$ est une base de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$, puisque E/F est modérément ramifiée, on a pour tout $\chi \in \hat{G}$:

$$\mathfrak{f}(\chi) = (a|\chi)(a|\bar{\chi}), \tag{4}$$

où $\bar{\chi}$ est le caractère conjugué de χ et $\mathfrak{f}(\chi)$ le conducteur du caractère χ ([5], chap. I, §6, theorem 7). En outre, E/F étant abélienne, on a :

$$D_{E/F} = \prod_{\chi \in \hat{G}} \mathfrak{f}(\chi) \tag{5}$$

([2], chap. II, §3, proposition 3.19 (a)). Or nous savons que :

$$\prod_{\chi \in \hat{G}} (a|\chi) = \prod_{\chi \in \hat{G}} (a|\bar{\chi}) \tag{6}$$

et par conséquent, de (4), (5) et (6) on obtient :

$$D_{E/F} = \Big(\prod_{\chi\in\hat{G}} (a|\chi)^2\Big)\,\mathfrak{O}_F. \tag{7}$$

Réciproquement, supposons que l'égalité (7) est vraie. On sait que sous les hypothèses de la proposition, on a :

$$D_{E/F}(\{a^g\}_{g\in G}) = \prod_{\chi\in\hat{G}} (a|\chi)^2 \tag{8}$$

([4], formule 1.3, p. 385), où $D_{E/F}(\{a^g\}_{g\in G}) = \det((\mathrm{Tr}_{E/F}(a^g a^{g'}))_{g,g'\in G})$. De (7) et (8) on déduit l'égalité d'idéaux :

$$D_{E/F}(\{a^g\}_{g\in G})\,\mathfrak{O}_F = D_{E/F}. \tag{9}$$

Par conséquent $\{a^g\}_{g\in G}$ est une base de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$ ([11], chap. III, §3). ■

Proposition 1.2. *Soit E/F une extension modérément ramifiée de corps de nombres de degré n, $\mathfrak{p}$ un idéal premier de F et $\mathfrak{p}\mathfrak{O}_E = \mathfrak{P}_1^{\alpha_1}\cdots\mathfrak{P}_r^{\alpha_r}$. Alors :*

$$v_{\mathfrak{p}}(D_{E/F}) = n - \sum_{i=1}^{r} f_i,$$

où f_i est le degré résiduel de $\mathfrak{P}_i$ dans E/F.

Il s'agit d'un cas particulier de la célèbre formule de Hilbert pour la valuation de la différente ([15], chap. IV, §1, proposition 4). ■

Soit l un nombre premier et ζ_l une racine primitive l-ième de l'unité dans $\mathbf{C}$.

Proposition 1.3. *Soit E/F une extension de Kummer de degré l, et soit $\alpha\in E$ tel que $E = F(\alpha)$ et $\alpha^l \in F$. Alors :*

i) l'extension E/F est modérément ramifiée si et seulement s'il existe $\beta\in F^*$ tel que $\beta^l\alpha^l \equiv 1 \mod {}^*(1-\zeta_l)^l$ (c'est à dire, $v_{\mathfrak{q}}(\beta^l\alpha^l - 1) \geq l\, v_{\mathfrak{q}}(1-\zeta_l)$ pour tout idéal premier $\mathfrak{q}$ de F divisant $(1-\zeta_l)$).

ii) si E/F est modérément ramifiée, les seuls idéaux premiers $\mathfrak{p}$ de F qui se ramifient dans E/F sont les idéaux $\mathfrak{p}$ tels que $v_{\mathfrak{p}}(\alpha^l\mathfrak{O}_F) = s$ avec $s\neq 0$ et $(s,l)=1$;

iii) l'extension E/F est non ramifiée si et seulement si E/F est modérément ramifiée et si $\alpha^l\mathfrak{O}_F = \mathfrak{a}^l$, où $\mathfrak{a}$ est un idéal fractionnaire de F.

[8], chap. V, §39, théorèmes 118 et 119. ■

2. Extensions de Kummer modérément ramifiées

On démontre dans ce paragraphe le théorème 2.1, énoncé dans l'introduction. Le théorème est vrai pour $l = 2$, mais pour des raisons techniques on va supposer dans la démonstration que $l > 2$. Le cas $l = 2$ est un exercice facile.

Soient $G = \mathrm{Gal}\,(E/F) = \{\sigma^i\}$ $(0 \le i \le l-1)$, χ_0 le caractère trivial de G et χ_1 le générateur de $\hat{G}$ défini par :

$$\chi_1(\sigma) = \zeta_l^{-1}, \tag{10}$$

où $\zeta_l = \exp(2\pi i/l)$. Supposons que $\{a^{\sigma^i}\}$ $(0 \le i \le l-1)$ est une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$. Posons :

$$\alpha_r = (a|\chi_1^r), \qquad 0 \le r \le l-1. \tag{11}$$

Alors $\alpha_r \in \mathfrak{O}_E$ $(0 \le r \le l-1)$. L'action galoisienne sur les résolvantes est donnée par :

$$(a|\chi_1^r)^\sigma = \zeta_l^{-r}(a|\chi_1^r), \qquad 0 \le r \le l-1. \tag{12}$$

On en déduit que $\alpha_r^\sigma = \zeta_l^{-r}\alpha_r$ $(0 \le r \le l-1)$. Par conséquent, $\alpha_r \in \mathfrak{O}_E$, $\alpha_r^l \in \mathfrak{O}_F$ et $E = F(\alpha_r)$ $(1 \le r \le l-1)$. Montrons que $\alpha = \alpha_1$ vérifie aussi les autres conditions qu'exige le théorème.

Puisque $\{a^{\sigma^i}\}$ $(0 \le i \le l-1)$ est une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$, on sait par la proposition 1.1 que :

$$D_{E/F} = (\prod_{r=0}^{l-1}(a|\chi_1^r)^2)\,\mathfrak{O}_F. \tag{13}$$

Puisque E/F est modérément ramifiée, l'on sait que $(a|\chi_0)$ est une unité de $\mathfrak{O}_F$. On a donc, de (13) :

$$D_{E/F} = (\prod_{r=1}^{l-1}\alpha_r^2)\,\mathfrak{O}_F. \tag{14}$$

Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ les idéaux premiers de $\mathfrak{O}_F$ qui se ramifient dans E/F; puisque l est premier, ils doivent être totalement ramifiés. Alors, d'après la formule de Hilbert (proposition 1.2) on a :

$$D_{E/F} = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^{l-1}. \tag{15}$$

Puisque $(\prod_{r=1}^{l-1} \alpha_r)^\sigma = \prod_{r=1}^{l-1} \zeta_l^{-r} \prod_{r=1}^{l-1} \alpha_r = \prod_{r=1}^{l-1} \alpha_r$, le produit $\prod_{r=1}^{l-1} \alpha_r$ appartient à $\mathfrak{O}_F$ et l'on déduit de (14) et (15) :

$$(\prod_{r=1}^{l-1} \alpha_r)\,\mathfrak{O}_F = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^{(l-1)/2}. \tag{16}$$

Si l'on prend la puissance l-ième dans (16), on obtient l'égalité suivante entre des idéaux de $\mathfrak{O}_F$:

$$\prod_{r=1}^{l-1} (\alpha_r^l\,\mathfrak{O}_F) = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^{l(l-1)/2}. \tag{17}$$

Soit $m_{r,j} = v_{\mathfrak{p}_j}(\alpha_r^l \mathfrak{O}_F)$. Alors, par le critère de ramification de Hecke (proposition 1.3 (ii)), on doit avoir $m_{r,j} > 0$ et $(m_{r,j}, l) = 1$, pour tout $r \in \{1, \dots, l-1\}$ et tout $j \in \{1, \dots, s\}$. De plus, pour chaque $j \in \{1, \dots, s\}$ fixé, on a grâce à (17) :

$$\sum_{r=1}^{l-1} m_{r,j} = l(l-1)/2. \tag{18}$$

Puisque $\alpha_r \alpha_{l-r} \in \mathfrak{O}_F$ pour $1 \leq r \leq (l-1)/2$, on peut donc écrire

$$m_{r,j} + m_{l-r,j} = l\,c_r, \tag{19}$$

avec $c_r \in \mathbf{Z}$ et $c_r \geq 1$ pour tout $r \in \{1, \dots, (l-1)/2\}$. On déduit de (18) et (19) :

$$\sum_{r=1}^{(l-1)/2} l\,c_r = l(l-1)/2. \tag{20}$$

Ou ce qui revient au même :

$$\sum_{r=1}^{(l-1)/2} c_r = (l-1)/2. \tag{21}$$

Cette égalité implique évidemment que $c_r = 1$ pour tout

$$r \in \{1, \dots, (l-1)/2\}.$$

On a donc $m_{r,j}+m_{l-r,j}=l$ pour tout $j\in\{1,\dots,s\}$ et tout $r\in\{1,\dots,(l-1)/2\}$; on en déduit que $0<m_{r,j}<l$ pour tout $j\in\{1,\dots,s\}$ et tout $r\in\{1,\dots,l-1\}$. Par conséquent, $\alpha_1^l\mathfrak{O}_F$ se décompose de manière unique sous la forme :

$$\alpha_1^l\mathfrak{O}_F=\prod_{i=1}^{l-1}\mathfrak{a}_i^i, \tag{22}$$

où les $\mathfrak{a}_i$ sont des idéaux entiers de F premiers entre eux et sans facteur carré. Plus généralement, on va étudier la décomposition de $\alpha_r^l\mathfrak{O}_F$ pour $r\in\{2,\dots,l-1\}$ par rapport à celle de $\alpha_1^l\mathfrak{O}_F$.

Soit $r\in\{1,\dots,l-1\}$; puisque $\alpha_1^{l-r}\alpha_r\in\mathfrak{O}_F$, on a :

$$v_{\mathfrak{p}_j}(\alpha_1^{l(l-r)}\alpha_r^l\mathfrak{O}_F)\in l\mathbf{Z},\qquad 1\le j\le s. \tag{23}$$

En outre :

$$v_{\mathfrak{p}_j}(\alpha_1^{l(l-r)})=m_{1,j}(l-r),\qquad v_{\mathfrak{p}_j}(\alpha_r^l)=m_{r,j},\qquad 1\le j\le s. \tag{24}$$

Donc, de (23) et (24) :

$$m_{r,j}+m_{1,j}(l-r)\in l\mathbf{Z},\qquad 1\le j\le s. \tag{25}$$

On peut alors montrer le lemme suivant :

Lemme.
On a l'égalité $m_{r,j}=rm_{1,j}-l[(r/l)m_{1,j}]$, $1\le j\le s$, $1\le r\le l-1$.

On déduit de (25) l'existence de $t\in\mathbf{Z}$ tel que :

$$m_{r,j}+m_{1,j}(l-r)=lt. \tag{26}$$

Puisque $0<m_{r,j}<l$, c'est que t est le plus grand entier tel que :

$$0<t<1+m_{1,j}-(r/l)m_{1,j}. \tag{27}$$

On en déduit l'égalité :

$$t=[1+m_{1,j}-(r/l)m_{1,j}]=1+m_{1,j}+[-(r/l)m_{1,j}]. \tag{28}$$

Or nous avons, puisque $(r/l)m_{1,j}$ n'est pas un entier, $1+[-(r/l)m_{1,j}]=-[(r/l)m_{1,j}]$, d'où $t=m_{1,j}-[(r/l)m_{1,j}]$ et donc l'égalité cherchée. ∎

On obtient du lemme :

$$\alpha_r^l \mathfrak{O}_F = (\alpha_1^l \mathfrak{O}_F)^r (\prod_{j=1}^{s} \mathfrak{p}_j^{-[(r/l)m_{1,j}]})^l, \qquad 1 \leq r \leq l-1. \tag{29}$$

En se reportant à la définition des idéaux $\mathfrak{a}_i$ et $\mathfrak{b}_r$ ((22) et (2)), on a :

$$\mathfrak{b}_r = \prod_{j=1}^{s} \mathfrak{p}_j^{[(r/l)m_{1,j}]}, \qquad 1 \leq r \leq l-1. \tag{30}$$

De (29) et (30) on déduit :

$$\alpha_r^l \mathfrak{O}_F = (\alpha_1^l \mathfrak{O}_F)^r \mathfrak{b}_r^{-l}, \qquad 1 \leq r \leq l-1. \tag{31}$$

On obtient ainsi que $\mathfrak{b}_r$ est principal, engendré par $x_r = \alpha_1^r/\alpha_r$. De plus, on a :

$$\begin{aligned} \sum_{j=1}^{l-1}(\alpha_1^j/x_j) &= \sum_{j=1}^{l-1} \alpha_j = (l-1)a + a^{\sigma}(\sum_{i=1}^{l-1} \zeta_l^i) + \cdots + a^{\sigma^{l-1}}(\sum_{i=1}^{l-1} \zeta_l^i) \\ &= (l-1)a - \sum_{i=1}^{l-1} a^{\sigma^i} = la - (a|\chi_0). \end{aligned} \tag{32}$$

Posons $x_0 = (a|\chi_0)^{-1}$; on rappelle que $(a|\chi_0) \in \mathfrak{O}_F^*$. On a donc, de (32) :

$$\sum_{j=0}^{l-1}(\alpha_1^j/x_j) \equiv 0 \mod l. \tag{33}$$

Ceci montre que $\alpha = \alpha_1$ vérifie toutes les propriétés exigées dans l'énoncé, et la première implication du théorème est donc démontrée.

Réciproquement, soit $\alpha \in \mathfrak{O}_E$ tel que $E = F(\alpha)$, $\alpha^l \in \mathfrak{O}_F$, et tel que $\alpha^l \mathfrak{O}_F = \prod_{i=1}^{l-1} \mathfrak{a}_i^i$ où les $\mathfrak{a}_i$ sont des idéaux de $\mathfrak{O}_F$ premiers entre eux et sans facteur carré, tels que les idéaux $\mathfrak{b}_j$ possèdent des générateurs x_j satisfaisant :

$$\sum_{j=0}^{l-1}(\alpha^j/x_j) \equiv 0 \mod l. \tag{34}$$

Soit $\sigma \in G$ défini par $\sigma(\alpha) = \zeta_l^{-1}\alpha$ (avec $\zeta_l = \exp(2\pi i/l)$) et soit $\chi_1 \in \hat{G}$ le caractère de G défini par $\chi_1(\sigma) = \zeta_l^{-1}$. On définit $a = \frac{1}{l}\sum_{j=0}^{l-1}(\alpha^j/x_j)$;

alors $a \in \mathfrak{O}_E$. On va démontrer que $\{a^{\sigma^i}\}$ $(0 \leq i \leq l-1)$ est une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.

Tout d'abord, on a $E = a\,F[G]$, puisque évidemment $\{\alpha^i\}$ $(0 \leq i \leq l-1)$ est une base de E sur F et la matrice de passage de $\{\alpha^i\}$ à $\{a^{\sigma^i}\}$ est une matrice dont le déterminant est un multiple non nul d'un déterminant de Vandermonde non nul. Grâce au critère de Fröhlich (proposition 1.1) il suffit de montrer que :

$$D_{E/F} = \prod_{\chi \in \hat{G}} (a|\chi)^2. \tag{35}$$

On a :

$$a^{\sigma^i} = (1/l) \sum_{j=0}^{l-1} \zeta_l^{-ij} (\alpha^j / x_j), \qquad 0 \leq i \leq l-1. \tag{36}$$

Par conséquent :

$$\begin{aligned} (a|\chi_0) &= \sum_{i=0}^{l-1} a^{\sigma^i} = (1/l) \sum_{i=0}^{l-1} \Big(\sum_{j=0}^{l-1} \zeta_l^{-ij} \alpha^j / x_j\Big) \\ &= (1/l) \sum_{j=0}^{l-1} (\alpha^j / x_j) \Big(\sum_{i=0}^{l-1} \zeta_l^{-ij}\Big) = (1/l) \sum_{j=0}^{l-1} (\alpha^j / x_j)(l\,\delta_{0,j}) \\ &= (1/l)(\alpha^0 / x_0)\, l = 1/x_0, \end{aligned} \tag{37}$$

et pour tout $r \in \{1, \ldots, l-1\}$, on a :

$$\begin{aligned} (a|\chi_1^r) &= \sum_{i=0}^{l-1} a^{\sigma^i} \chi_1^r(\sigma^{-i}) = \sum_{i=0}^{l-1} a^{\sigma^i} \zeta_l^{ri} = (1/l) \sum_{i=0}^{l-1} \Big(\sum_{j=0}^{l-1} \zeta_l^{-ij} \alpha^j / x_j\Big) \zeta_l^{ri} \\ &= (1/l) \sum_{j=0}^{l-1} (\alpha^j / x_j) \Big(\sum_{i=0}^{l-1} \zeta_l^{i(r-j)}\Big) = (1/l) \sum_{j=0}^{l-1} (\alpha^j / x_j)(l\,\delta_{r,j}) \\ &= (1/l)(\alpha^r / x_r)\, l = \alpha^r / x_r. \end{aligned} \tag{38}$$

On a donc, de (37) et (38) :

$$\prod_{\chi \in \hat{G}} (a|\chi)^2 = \prod_{r=0}^{l-1} (a|\chi_1^r)^2 = \prod_{r=0}^{l-1} (\alpha^r / x_r)^2 \tag{39}$$

$$= (\alpha^{l(l-1)/2})^2/(x_0x_1\cdots x_{l-1})^2 = \alpha^{l(l-1)}/(x_0x_1\cdots x_{l-1})^2.$$

De l'égalité :

$$\sum_{k=1}^{l-1}[ki/l] = (i-1)(l-1)/2, \qquad 1 \le i \le l-1, \tag{40}$$

on déduit :

$$(\mathfrak{b}_0\cdots\mathfrak{b}_{l-1})^{-2}\prod_{i=1}^{l-1}\mathfrak{a}_i^{i(l-1)} = \prod_{i=1}^{l-1}\mathfrak{a}_i^{l-1}, \tag{41}$$

et par conséquent, de (39) et (41) :

$$\Big(\prod_{\chi\in\hat{G}}(a|\chi)^2\Big)\,\mathfrak{O}_F = \Big(\prod_{i=1}^{l-1}\mathfrak{a}_i\Big)^{l-1}. \tag{42}$$

Déterminons maintenant le discriminant $D_{E/F}$. Soient $\mathfrak{p}_1,\ldots,\mathfrak{p}_s$ les idéaux premiers de $\mathfrak{O}_F$ qui divisent $\alpha^l\mathfrak{O}_F$, c'est à dire, exactement les diviseurs des $\mathfrak{a}_i$ $(1 \le i \le l-1)$. D'après le critère de ramification de Hecke (proposition 1.3 (ii)), les idéaux $\mathfrak{p}_1,\ldots,\mathfrak{p}_s$ sont les seuls idéaux premiers qui se ramifient dans l'extension E/F. Ils doivent se ramifier totalement, donc, grâce à la formule de Hilbert (proposition 1.2), on a :

$$v_{\mathfrak{p}_i}(D_{E/F}) = l-1, \qquad 1 \le i \le s, \tag{43}$$

et par conséquent :

$$D_{E/F} = (\mathfrak{p}_1\cdots\mathfrak{p}_s)^{l-1}. \tag{44}$$

Mais $\mathfrak{p}_1,\ldots,\mathfrak{p}_s$ étant exactement les idéaux premiers qui divisent les $\mathfrak{a}_i$, on a aussi :

$$\Big(\prod_{i=1}^{l-1}\mathfrak{a}_i\Big)^{l-1} = (\mathfrak{p}_1\cdots\mathfrak{p}_s)^{l-1}. \tag{45}$$

On déduit de (42), (44) et (45) :

$$D_{E/F} = \Big(\prod_{\chi\in\hat{G}}(a|\chi)^2\Big)\mathfrak{O}_F, \tag{46}$$

et $\{a^{\sigma^i}\}$ $(0 \leq i \leq l-1)$ est une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$. Le théorème est démontré. ■

Remarque 2.2 On remarque que s'il existe α satisfaisant les conditions du théorème, alors il existe aussi β satisfaisant les conditions et en outre $\beta \equiv 1 \mod (1-\zeta_l)$. En effet, si α satisfait les conditions du théorème et l'on pose $a = (1/l)\sum_{j=0}^{l-1}(\alpha^j/x_j)$, alors $\{a^{\sigma^i}\}$ est une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$, donc $\beta = (a|\chi_1)/(a|\chi_0)$ satisfait les mêmes propriétés que α et en outre :

$$\begin{aligned}\beta &= (a|\chi_1)/(a|\chi_0) = (\sum_{i=0}^{l-1} a^{\sigma^i}\chi_1(\sigma^{-i}))/(a|\chi_0) \\ &= ((a|\chi_0) + \sum_{i=0}^{l-1} a^{\sigma^i}(\zeta_l^i - 1))/(a|\chi_0) = 1 + x\,(1-\zeta_l)\end{aligned} \tag{47}$$

avec $x \in \mathfrak{O}_E$, puisque $(1-\zeta_l^i)\mathfrak{O}_F = (1-\zeta_l)\mathfrak{O}_F$ pour $1 \leq i \leq l-1$. On a donc $\beta \equiv 1 \mod (1-\zeta_l)$. Plus généralement, on montre de façon analogue que si l'on pose $\beta_r = (a|\chi_r)/(a|\chi_0)$, on a $\beta_r \equiv 1 \mod (1-\zeta_l)$ pour $1 \leq r \leq l-1$.

Remarque 2.3 Quitte à remplacer α par $\alpha' = \alpha x_0/x_1$ et les x_j par $x'_j = x_j x_0^{j-1}/x_1^j$ pour $2 \leq j \leq l-1$, on peut toujours supposer que $x_0 = x_1 = 1$ dans l'énoncé du théorème.

Remarque 2.4 Avec les notations du théorème, on remarque que si $x_j \equiv 1 \mod l$ $(0 \leq j \leq l-1)$, alors $\sum_{j=0}^{l-1}(\alpha^j/x_j) \equiv \sum_{j=0}^{l-1}\alpha^j \mod l$. Si en outre $\alpha \equiv 1 \mod (1-\zeta_l)$, on obtient $\sum_{j=0}^{l-1}\alpha^j \equiv 0 \mod l$. Ainsi, $\alpha \equiv 1 \mod (1-\zeta_l)$ et $x_j \equiv 1 \mod l$ $(0 \leq j \leq l-1)$ impliquent $\sum_{j=0}^{l-1}(\alpha^j/x_j) \equiv 0 \mod l$.

Il est intéressant d'énoncer le théorème 2.1 d'une autre manière qui montre la symétrie du rôle que jouent les α_r qui apparaissent dans la démonstration. Si E/F est une extension de Kummer de degré premier l, appellons famille complète de générateurs entiers de Kummer de E/F toute famille $\{\gamma_j\}$ $(1 \leq j \leq l-1)$ d'éléments de $\mathfrak{O}_E$ tels que $E = F(\gamma_j)$, $\gamma_j^l \in \mathfrak{O}_F$ et les γ_j^l représentent toutes les classes non triviales du groupe $(F^* \cap E^{*l})/F^{*l}$, c'est à dire les classes associées à l'extension E/F. On dit qu'un idéal entier $\mathfrak{a}$ de $\mathfrak{O}_F$ est sans puissance l-ième si $v_{\mathfrak{p}}(\mathfrak{a}) < l$ pour tout idéal premier $\mathfrak{p}$ de $\mathfrak{O}_F$. Le théorème 2.1 s'énonce alors de la façon suivante :

Théorème 2.1 (bis). *Soit E/F une extension de Kummer modérément ramifiée de degré l premier. Alors $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$ si et seulement s'il existe une famille complète $\{\gamma_j\}$ de générateurs entiers de*

Kummer de E sur F telle que :

i) les idéaux $\gamma_j^l\mathfrak{O}_F$ sont sans puissance l-ième,

ii) on a la congruence : $\sum_{j=0}^{l-1}\gamma_j \equiv 0 \mod l$ (avec $\gamma_0 = 1$).

En outre dans ce cas $(1/l)\sum_{j=0}^{l-1}\gamma_j$ engendre une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$.

Soient α et x_j ($0 \leq j \leq l-1$) qui vérifient les conditions du théorème 2.1. Alors $\gamma_j = \alpha^j/x_0x_j$ ($1 \leq j \leq l-1$) vérifient les conditions du théorème 2.1 (bis).

Réciproquement, soit $\{\gamma_j\}$ ($1 \leq j \leq l-1$) une famille qui vérifie les conditions du théorème 2.1 (bis). On peut supposer, en réordonnant les γ_j si nécessaire, que $\gamma_1^j/\gamma_j \in F^*$. Soit $\mathfrak{a} = \gamma_1^l\mathfrak{O}_F = \prod_{i=1}^{l-1}\mathfrak{a}_i^i$, avec les $\mathfrak{a}_i$ des idéaux entiers de F premiers entre eux et sans facteur carré, et soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ les idéaux premiers de F qui ramifient dans l'extension E/F; posons $m_{j,i} = v_{\mathfrak{p}_i}(\gamma_j^l\mathfrak{O}_F)$ ($1 \leq j \leq l-1$, $1 \leq i \leq s$). Maintenant, le même raisonnement qu'on a fait dans la démonstration du théorème 2.1 montre que $\gamma_j^l\mathfrak{O}_F = \mathfrak{b}_j^{-l}\prod_{i=1}^{l-1}\mathfrak{a}_i^{ji}$ ($1 \leq j \leq l-1$), où les $\mathfrak{b}_j$ sont les idéaux associés à $\mathfrak{a}$. En particulier, les idéaux $\mathfrak{b}_j$ sont principaux, engendrés par γ_1^j/γ_j. On en déduit que $\alpha = \gamma_1$ et $x_j = \gamma_1^j/\gamma_j$ ($0 \leq j \leq l-1$) satisfont les conditions du théorème 2.1. ∎

Soit E/F une extension de corps de nombres de degré fini n. On sait que si $\{\alpha_1, \ldots, \alpha_n\}$ est une F-base de E, alors il existe un idéal fractionnaire B de F tel que :

$$D_{E/F} = B^2(d(\alpha_1, \ldots, \alpha_n)\mathfrak{O}_F) \tag{48}$$

où $d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{E/F}(\alpha_i\alpha_j))$. On appelle *classe de Steinitz* de l'extension E/F la classe de l'idéal B dans le groupe de classes $\mathrm{Cl}(F)$; on voit aisément que cette définition ne dépend pas de la F-base de E choisie. On sait qu'en général $\mathfrak{O}_E$ n'est pas $\mathfrak{O}_F$-libre; Emil Artin ([1]) a montré que $\mathfrak{O}_E$ est $\mathfrak{O}_F$-libre si et seulement si la classe de Steinitz de E/F est triviale. La proposition suivante aide à mieux interpréter le théorème 2.1.

PROPOSITION 2.5. *Soit E/F une extension de Kummer modérément ramifiée de degré l premier. Supposons qu'il existe $\alpha \in \mathfrak{O}_E$ tel que $\alpha^l \in \mathfrak{O}_F$, $E = F(\alpha)$, et $\mathfrak{a} = \alpha^l\mathfrak{O}_F$ est sans puissance l-ième; soient $\mathfrak{b}_j$ ($0 \leq j \leq l-1$) les idéaux associés à $\mathfrak{a}$. Alors $\mathfrak{O}_E$ est $\mathfrak{O}_F$-libre si et seulement si l'idéal $\prod_{j=0}^{l-1}\mathfrak{b}_j$ est principal.*

On va faire la démonstration pour $l > 2$; pour $l = 2$, il s'agit d'un exercice facile. Soit $\alpha^l\mathfrak{O}_F = \prod_{i=1}^{l-1}\mathfrak{a}_i^i$ avec les $\mathfrak{a}_i$ des idéaux premiers entre eux et sans facteur carré. Puisque l'extension E/F est modérément ramifiée, on a d'une part :

(49) $$D_{E/F} = (\prod_{i=1}^{l-1} \mathfrak{a}_i)^{l-1}.$$

D'autre part, on obtient en utilisant la formule d'Euler ([14], chap. II, §7, formule 6) :

(50) $$d(1, \alpha, \ldots, \alpha^{l-1}) = l^l \alpha^{l(l-1)}.$$

Appellons B le seul idéal fractionnaire de F tel que :

(51) $$(\prod_{i=1}^{l-1} \mathfrak{a}_i)^{l-1} = B^2 l^l (\prod_{i=1}^{l-1} \mathfrak{a}_i^i)^{l-1}.$$

On a donc :

(52) $$(\prod_{i=1}^{l-1} \mathfrak{a}_i)^{(l-1)/2} = B(1-\zeta_l)^{l(l-1)/2} (\prod_{i=1}^{l-1} \mathfrak{a}_i^i)^{(l-1)/2}.$$

Mais, par définition des $\mathfrak{b}_j$ $(0 \leq j \leq l-1)$, on a :

(53) $$(\prod_{i=1}^{l-1} \mathfrak{a}_i)^{(l-1)/2} \prod_{j=0}^{l-1} \mathfrak{b}_j = (\prod_{i=1}^{l-1} \mathfrak{a}_i^i)^{(l-1)/2}.$$

On déduit de (52) et (53) :

(54) $$B((1-\zeta_l)^{l(l-1)/2} \mathfrak{O}_F) \prod_{j=0}^{l-1} \mathfrak{b}_j = \mathfrak{O}_F.$$

Par conséquent, la classe de Steinitz de l'extension E/F est la classe de l'idéal $(\prod_{j=1}^{l-1} \mathfrak{b}_j)^{-1}$. D'après le résultat d'Artin cité ci-dessus, $\mathfrak{O}_E$ est $\mathfrak{O}_F$-libre si et seulement si l'idéal $\prod_{j=1}^{l-1} \mathfrak{b}_j$ est principal. ∎

COROLLAIRE 2.6. *Soit E/F une extension de Kummer modérément ramifiée de degré l premier. S'il existe $\alpha \in \mathfrak{O}_E$ tel que $\alpha^l \in \mathfrak{O}_F$, $E = F(\alpha)$, $\mathfrak{a} = \alpha^l \mathfrak{O}_F$ est sans puissance l-ième et les idéaux $\mathfrak{b}_j$ $(0 \leq j \leq l-1)$ associés à $\mathfrak{a}$ sont principaux, alors $\mathfrak{O}_E$ est $\mathfrak{O}_F$-libre.* ■

Remarque 2.7 La réciproque du corollaire 2.6 est vraie pour $l = 2$. Autrement dit, on peut montrer aisément que si E est une extension quadratique et modérément ramifiée de F, alors $\mathfrak{O}_E$ est $\mathfrak{O}_F$-libre si et seulement s'il existe $\alpha \in \mathfrak{O}_E$ tel que $\alpha^2 \in \mathfrak{O}_F$, $E = F(\alpha)$ et $\alpha^2 \mathfrak{O}_F$ est un idéal sans facteur carré. Il s'agit d'un cas particulier d'un théorème démontré par H. B. Mann ([12], theorem 2, p. 170).

Le reste de ce paragraphe est consacré à démontrer quelques lemmes qu'on va utiliser dans le §4 et à examiner quelques exemples.

LEMME 2.8. *Soit E un corps de nombres qui contient ζ_l et tel que, pour tout idéal premier $\mathfrak{p}$ de E, on ait $v_{\mathfrak{p}}(1-\zeta_l) \leq 1$. Soient x et z des entiers de E, premiers avec $(1-\zeta_l)$. Alors $x \equiv z \mod (1-\zeta_l)$ si et seulement si $x^l \equiv z^l \mod (1-\zeta_l)^l$.*

La fonction f de $H_1 = (\mathfrak{O}_E/(1-\zeta_l)\mathfrak{O}_E)^*$ dans $H_2 = (\mathfrak{O}_E/(1-\zeta_l)^l \mathfrak{O}_E)^{*l}$ définie par $f(\alpha + (1-\zeta_l)\mathfrak{O}_E) = \alpha^l + (1-\zeta_l)^l \mathfrak{O}_E$ est un homomorphisme de groupes bien défini et surjectif. Soit $(1-\zeta_l)\mathfrak{O}_E = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, où les $\mathfrak{p}_i$ $(1 \leq i \leq s)$ sont des idéaux premiers distincts de $\mathfrak{O}_E$. L'ordre du groupe H_1 est égal à $\Phi(\mathfrak{p}_1 \cdots \mathfrak{p}_s) = \prod_{i=1}^{s} (\mathbf{N}(\mathfrak{p}_i) - 1)$ et l'ordre du groupe H_2 est un diviseur de $\Phi(\mathfrak{p}_1^l \cdots \mathfrak{p}_s^l) = \prod_{i=1}^{s} \mathbf{N}(\mathfrak{p}_i)^{l-1}(\mathbf{N}(\mathfrak{p}_i) - 1)$. Puisque l ne divise pas $(\mathbf{N}(\mathfrak{p}_i) - 1)$ $(1 \leq i \leq s)$, l'ordre de H_2 est supérieur ou égal à $\prod_{i=1}^{s} (\mathbf{N}(\mathfrak{p}_i) - 1)$, donc égal à l'ordre de H_1. On en déduit que f est un isomorphisme de groupes. ■

On note $\mathbf{C}_n$ le groupe cyclique à n éléments.

LEMME 2.9. *Soit l un nombre premier, $F = \mathbf{Q}(\zeta_l)$ le l-ième corps cyclotomique et $G = (\mathfrak{O}_F/(1-\zeta_l)^l \mathfrak{O}_F)^*$. Alors $G \simeq \mathbf{C}_l \times \cdots \times \mathbf{C}_l \times \mathbf{C}_{l-1}$.*

Puisque $\mathfrak{p} = (1-\zeta_l)$ est un idéal maximal de $\mathfrak{O}_F$, on sait que $|G| = \Phi(\mathfrak{p}^l) = (l-1)l^{l-1}$. On a la suite exacte :

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{j} U \longrightarrow 1, \tag{55}$$

où U est le groupe $(\mathfrak{O}_F/(1-\zeta_l)\mathfrak{O}_F)^*$ et j est induit par la surjection canonique. Puisque $|H|$ et $|U|$ sont premiers entre eux, le groupe G est produit direct de H par U. Le groupe U est cyclique d'ordre $l-1$ et G est le l-sous-groupe de Sylow de G. Tout élément de H est représenté par un élément x de $\mathfrak{O}_F$, $x \equiv 1 \mod (1-\zeta_l)$. Puisque $x^l \equiv 1 \mod (1-\zeta_l)^l$, on en déduit que H est d'exposant l, d'où le résultat. ■

PROPOSITION 2.10. *Soit l un nombre premier, $F = \mathbf{Q}(\zeta_l)$ et E une extension modérément ramifiée de F de degré l. Supposons que E possède un générateur de Kummer $\gamma \in \mathfrak{O}_E$ tel que $v_{\mathfrak{p}}(\gamma^l \mathfrak{O}_F) < l$ pour tout idéal premier $\mathfrak{p}$ de F. Alors E possède un générateur de Kummer $\alpha \in \mathfrak{O}_E$ tel que $v_{\mathfrak{p}}(\alpha^l \mathfrak{O}_F) < l$ pour tout idéal premier $\mathfrak{p}$ de F et $\alpha \equiv 1 \mod (1-\zeta_l)$.*

Puisque E/F est modérément ramifiée, le critère de ramification de Hecke (proposition 1.3) assure l'existence de $\beta \in F^*$ tel que $\beta^l\gamma^l \equiv 1 \mod {}^*(1-\zeta_l)^l$. Puisque $v_{\mathfrak{p}}(\gamma^l\mathfrak{O}_F) < l$ pour tout idéal premier $\mathfrak{p}$ de F, l'idéal $\gamma^l\mathfrak{O}_F$ est premier avec l. Donc β est premier avec l et par conséquent il définit un élément de $\mathfrak{O}_{F,\mathfrak{p}}^*$ (avec $\mathfrak{p} = (1-\zeta_l)$). Donc dans $\mathfrak{O}_{F,\mathfrak{p}}$ on a $\beta^l\gamma^l \equiv 1 \mod (1-\zeta_l)^l$ si et seulement si $\gamma^l \equiv \beta^{-l} \mod (1-\zeta_l)^l$. Mais $(\mathfrak{O}_{F,\mathfrak{p}}/\mathfrak{p}\mathfrak{O}_{F,\mathfrak{p}})^* \simeq (\mathfrak{O}_F/\mathfrak{p})^*$, donc il existe $x \in \mathfrak{O}_F$ tel que $\beta^{-1} \equiv x \mod (1-\zeta_l)$, c'est à dire, $\beta^{-l} \equiv x^l \mod (1-\zeta_l)^l$. Donc il est clair qu'il existe $x \in \mathfrak{O}_F$, x premier avec l, tel que :

$$\gamma^l \equiv x^l \mod (1-\zeta)^l. \tag{56}$$

On en déduit la congruence (lemme 2.8) :

$$\gamma \equiv x \mod (1-\zeta_l). \tag{57}$$

Il suffit pour achever la démonstration de montrer l'existence de $u \in \mathfrak{O}_F^*$ tel que :

$$\gamma \equiv u \mod (1-\zeta_l), \tag{58}$$

puisque alors $\alpha = \gamma u^{-1}$ satisfera les conditions de la proposition. Il suffit donc de montrer que le groupe :

$$(\mathfrak{O}_F/(1-\zeta_l)\mathfrak{O}_F)^*/\mathrm{Im}(\mathfrak{O}_F^*) \tag{59}$$

est réduit à $\{1\}$. Puisque l'idéal $(1-\zeta_l)$ est totalement ramifié dans $F/\mathbf{Q}$, le groupe $(\mathfrak{O}_F/(1-\zeta_l)\mathfrak{O}_F)^*$ est cyclique d'ordre $l-1$. Pour tout entier a, $1 \le a \le l-1$, on pose $u_a = (\zeta_l^a - 1)/(\zeta_l - 1)$; c'est une unité de $\mathfrak{O}_F$. Puisque $u_a \equiv a \mod (1-\zeta_l)$, les unités u_a définissent $l-1$ classes distinctes modulo $(1-\zeta_l)$, d'où le résultat. ∎

Pour les extensions quadratiques, on obtient grâce au théorème 2.1 le résultat suivant :

Proposition 2.11. *Soit E/F une extension quadratique. Alors $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$ si et seulement s'il existe $\alpha \in \mathfrak{O}_E$ tel que $E = F(\alpha)$, $\alpha^2 \in \mathfrak{O}_F$, $\alpha \equiv 1 \mod 2$ et $\alpha^2\mathfrak{O}_F$ est un idéal de $\mathfrak{O}_F$ sans facteur carré.* ∎

Remarque 2.12 On peut utiliser ce critère pour montrer que si K est un corps quadratique imaginaire de discriminant d_K égal à -8, -11, -19, -43, -67 ou -163, il existe une infinité d'idéaux premiers $\mathfrak{p}$ de K tels que l'anneau des entiers de $K(\mathfrak{p})$, le corps de classes de rayon de K de conducteur $\mathfrak{p}$, ne possède pas une base normale sur $\mathfrak{O}_K$ ([6], chap. II, [7]).

Pour les extensions de Kummer cubiques, le théorème 2.1 peut s'énoncer de la façon suivante :

Proposition 2.13. *Soit E/F une extension de Kummer cubique. Alors $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$ si et seulement s'il existe $\alpha \in \mathfrak{O}_E$ tel que $\alpha^3 \in \mathfrak{O}_F$, $E = F(\alpha)$, $\alpha \equiv 1 \mod (1-\zeta_3)$, $\alpha^3\mathfrak{O}_F = \mathfrak{a}\mathfrak{b}^2$ où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux premiers entre eux et sans facteur carré, et $\mathfrak{b}$ est un idéal principal engendré par x tel que $x \equiv 1 \mod 3$.*

Posons $w = \zeta_3$. Grâce au théorème 2.1 et aux remarques 2.2 et 2.3, il suffit de montrer que si $\alpha \in \mathfrak{O}_E$ est tel que $\alpha^3 \in \mathfrak{O}_F$, $E = F(\alpha)$, $\alpha \equiv 1 \mod (1-\omega)$, $\alpha^3\mathfrak{O}_F = \mathfrak{a}\mathfrak{b}^2$ où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux premiers entre eux et sans facteur carré, et $\mathfrak{b}$ est un idéal principal engendré par x, alors $1 + \alpha + (\alpha^2/x) \equiv 0 \mod 3$ si et seulement si $x \equiv 1 \mod 3$.

En effet, puisque $\alpha \equiv 1 \mod (1-\omega)$, on a $1 + \alpha + \alpha^2 \equiv 0 \mod 3$. Donc il est clair que si $x \equiv 1 \mod 3$, alors $1 + \alpha + (\alpha^2/x) \equiv 0 \mod 3$. Réciproquement, si $1 + \alpha + (\alpha^2/x) \equiv 0 \mod 3$, alors on a $(\alpha^2/x) \equiv \alpha^2 \mod 3$, ou ce qui revient au même, $\alpha^2 \equiv x\alpha^2 \mod 3$; puisque α^2 est inversible modulo 3, on en déduit que $x \equiv 1 \mod 3$. ∎

Exemple 2.14 Toute extension cubique E modérément ramifiée de $\mathbf{Q}(\omega)$ est telle que $\mathfrak{O}_E$ possède une base normale sur $\mathbf{Z}[\omega]$. En effet, puisque $\mathbf{Z}[\omega]$ est principal, toute extension cubique modérément ramifiée E de $\mathbf{Q}(\omega)$ possède un générateur de Kummer $\alpha \in \mathfrak{O}_E$ tel que $\alpha^3\mathbf{Z}[\omega]$ est sans puissance cubique. D'après la proposition 2.10, on peut supposer que $\alpha \equiv 1 \mod (1-\omega)$. Notre assertion sera démontrée s'il est vrai que tout idéal $\mathfrak{b}$ de $\mathbf{Z}[\omega]$, premier avec 3, possède un générateur $x \equiv 1 \mod 3$; ou ce qui revient au même, que le groupe $(\mathbf{Z}[\omega]/3\mathbf{Z}[\omega])^*/\mathrm{Im}(\mathbf{Z}[\omega]^*)$ est trivial. Mais $\Phi(3\mathbf{Z}[\omega]) = \mathrm{N}(1-\omega)(\mathrm{N}(1-\omega)-1) = 3\cdot 2 = 6$ et $\mathbf{Z}[\omega]^* = \{\pm 1, \pm\omega, \pm\omega^2\}$; on vérifie facilement que les six unités de $\mathbf{Z}[\omega]$ sont non congrues modulo 3.

3. Extensions de Kummer non ramifiées

Si l'on examine la démonstration du théorème 2.1 lorsqu'on suppose que l'extension E/F est non ramifiée, on obtient le théorème suivant :

PROPOSITION 3.1. *Soit E/F une extension de Kummer non ramifiée de degré l premier. Alors, il existe une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$ si et seulement s'il existe $v \in \mathfrak{O}_E^*$ tel que $E = F(v)$, $v^l \in \mathfrak{O}_F^*$ et $v \equiv 1 \mod (1-\zeta_l)$. Dans ce cas, une base normale est donnée par $(1/l)(1+v+\cdots+v^{l-1})$ et ses conjugués.* ∎

Conséquence 3.2 Soit E/F une extension de Kummer non ramifiée de degré l premier. On dit que $\alpha \in \mathfrak{O}_E$ est un générateur kummerien de E/F lorsque $E = F(\alpha)$ et $\alpha^l \in \mathfrak{O}_F$. Alors, il y a trois possibilités :
1) il n'existe pas de générateur kummerien $\alpha \in \mathfrak{O}_E$ de E/F tel que α soit une unité. Dans ce cas, $\mathfrak{O}_E$ ne possède pas de base normale sur $\mathfrak{O}_F$,
2) il existe un générateur kummerien $\alpha \in \mathfrak{O}_E$ de E/F tel que α soit une unité de $\mathfrak{O}_E$, mais l'on a $\alpha u \not\equiv 1 \mod (1-\zeta_l)$ pour tout $u \in \mathfrak{O}_F^*$. Dans ce cas, $\mathfrak{O}_E$ ne possède pas de base normale sur $\mathfrak{O}_F$,
3) il existe un générateur kummerien $v \in \mathfrak{O}_E^*$ de E/F tel que $v \equiv 1 \mod (1-\zeta_l)$. Alors $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$. Dans ce cas, $(1/l)(1+v+\cdots+v^{l-1})$ engendre une telle base.

Remarque 3.3 Si l'idéal $(1-\zeta_l)$ est non ramifié dans $F/\mathbf{Q}(\zeta_l)$ (et par conséquent, aussi dans $E/\mathbf{Q}(\zeta_l)$), le cas 2) est impossible. En effet, le groupe $(\mathfrak{O}_E/(1-\zeta_l)\mathfrak{O}_E)^*$ étant d'ordre premier à l, on peut toujours obtenir à partir d'un générateur kummerien $v \in \mathfrak{O}_E^*$ de E/F un autre générateur kummerien $v' \in \mathfrak{O}_E^*$ de E/F tel que $v' \equiv 1 \mod (1-\zeta_l)$, en posant $v' = v^m$ pour un m convenable. Plus précisement, on peut prendre m égal à l'exposant du groupe $(\mathfrak{O}_E/(1-\zeta_l)\mathfrak{O}_E)^*$. Dans ce cas, donc, il existe une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$ si et seulement s'il existe un générateur kummerien $v \in \mathfrak{O}_E$ de E/F tel que $v \in \mathfrak{O}_E^*$.

On peut interpréter nos résultats de la manière suivante : soit $\mathcal{F}_l(F)$ (resp. $\mathcal{E}_l(F)$, resp. $\mathcal{E}_l'(F)$) les extensions (resp. extensions modérément ramifiées, resp. extensions non ramifiées) de F, cycliques de degré l, contenues dans $\bar{F}$. L'application :

$$\theta_F\colon F^*/F^{*l} \longrightarrow \mathcal{F}_l(F) \tag{60}$$

définie par $\alpha F^{*l} \mapsto F(\alpha^{1/l})$, est une aplication surjective.
Soit $\mathfrak{f} = (1-\zeta_l)\mathfrak{O}_F$ et soit M_F l'ensemble des idéaux premiers de $\mathfrak{O}_F$. On pose :

$$U_{\mathfrak{f}} = \{x \in F^* \mid x \equiv 1 \mod {}^*\mathfrak{f}^l\}, \tag{61}$$

$$V_{\mathfrak{f}} = \{x \in F^* \mid x \in F_{\mathfrak{p}}^{*\,l}(1 + \mathfrak{f}^l \mathfrak{O}_{F,\mathfrak{p}}),\ \ \forall \mathfrak{p} \in M_F\}. \tag{62}$$

Lorsque $\mathfrak{p}$ ne divise pas $\mathfrak{f}$, $1 + \mathfrak{f}^l \mathfrak{O}_{F,\mathfrak{p}}$ doit être compris comme $\mathfrak{O}_{F,\mathfrak{p}}^*$.

La proposition 1.3 est équivalente à :

$$\theta_F^{-1}(\mathcal{E}_l(F)) = U_{\mathfrak{f}} F^{*\,l} / F^{*\,l} \tag{63}$$

et

$$\theta_F^{-1}(\mathcal{E}'_l(F)) = V_{\mathfrak{f}} / F^{*\,l}. \tag{64}$$

L'égalité (64) est en fait le théorème 11 de [18]. Lorsque E/F est non ramifiée de groupe de Galois G, on peut vérifier que 3.2 (1) signifie que l'anneau des entiers de E étendu à l'ordre maximal $\mathcal{M}$ de $F[G]$ n'est pas libre sur cet ordre. Dans le cas 3.2 (2), $\mathfrak{O}_E$ étendu à $\mathcal{M}$ est libre sur $\mathcal{M}$ mais n'est pas libre sur $\mathfrak{O}_F[G]$. Dans le cas 3.2 (3), $\mathfrak{O}_E$ est libre sur $\mathfrak{O}_F[G]$.

Si l'on désigne par $\operatorname{Ker}\psi$ l'ensemble des éléments de $\theta_F^{-1}(\mathcal{E}'_l(F))$ pour lesquels l'extension E/F associée possède un anneau d'entiers à base normale sur $\mathfrak{O}_F$, la proposition 3.1 nous donne l'égalité :

$$\operatorname{Ker}\psi = Y_{\mathfrak{f}} F^{*\,l} / F^{*\,l} \tag{65}$$

où $Y_{\mathfrak{f}} = \{x \in \mathfrak{O}_F^* \mid x \equiv 1 \mod \mathfrak{f}^l\}$. C'est encore le théorème 11 de [18].

Soit maintenant l un nombre premier et $F = \mathbf{Q}(\zeta_l)$. Les extensions non ramifiées de degré l de F dont l'anneau des entiers possède une base normale sur $\mathfrak{O}_F$, d'après ce qui précède, sont décrites par le groupe $G = Y_{\mathfrak{f}}/(F^{*\,l} \cap Y_{\mathfrak{f}})$. Ce groupe est un groupe fini annulé par l et sur lequel agit $\Delta = \operatorname{Gal}(F/\mathbf{Q})$, donc il possède une structure naturelle de $\mathbf{Z}_l[\Delta]$-module. Il existe un lien entre la structure de G comme $\mathbf{Z}_l[\Delta]$-module et la valeur en 1 d'une certaine fonction L l-adique. Plus précisément, pour chaque $i \in \{0, \dots, l-2\}$, soit G_i (resp. H_i) la i-partie de la décomposition de G (resp. du l-sous-groupe de Sylow de $\operatorname{Cl}(F)$) comme $\mathbf{Z}_l[\Delta]$-module suivant les idempotents primitifs de $\mathbf{Z}_l[\Delta]$ et soit h_i le cardinal de H_i. Pour chaque caractère $\chi \neq 1$ de $(\mathbf{Z}/l\mathbf{Z})^*$, soit $L_l(s,\chi)$ la fonction L l-adique associée à χ ([19], chap. V, §5.2, theorem 5.11); soit ϕ le caractère de Teichmüller de $(\mathbf{Z}/l\mathbf{Z})^*$. Alors, on a ([18], chap. IV, theorem 14) :

Théorème 3.4. *(M. J. Taylor) Soit $i \in \{0, \dots, l-2\}$. Alors :*
a) Si $i = 0$ ou i impair, $G_i = 0$.
b) Si i est pair, $i \neq 0$, alors $G_i = 0$ si et seulement si $L_l(1,\phi^i)/h_i \not\equiv 0 \mod l$.

Ce qu'on veut préciser ici est le fait que sous la conjecture de Vandiver (c'est à dire, lorsque l ne divise pas le nombre de classes de $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$), on peut construire explicitement une base normale de $\mathfrak{O}_L$ sur $\mathfrak{O}_F$ pour toute extension L de F cyclique de degré l et non ramifiée. Tout ce qui suit est démontré dans [19], en particulier dans le chapitre 8.

Supposons donc que l satisfait la conjecture de Vandiver; on sait que tout premier $l \leq 125000$ la satisfait. On dit que l est irrégulier si l divise le nombre de classes de F, régulier sinon; il est clair que si l est régulier, alors $G = 0$. D'après un critère célèbre de Kummer, l est irrégulier si et seulement s'il existe $k \in \{2, 4, \ldots, l-3\}$ tel que l divise le nombre de Bernoulli B_k. Les entiers $i_1 < i_2 < \cdots < i_s$ tels que $i_j \in \{2, 4, \ldots, l-3\}$ $(1 \leq j \leq s)$ et l divise B_{i_j} s'appellent les indices d'irrégularité pour l; dire que l est irrégulier équivaut à dire que $s \geq 1$. Le plus petit premier irrégulier est $l = 37$; le plus petit premier irrégulier avec $s > 1$ est $l = 157$.

On peut démontrer que le l-rang de $\mathrm{Cl}(F)$ est supérieur ou égal à s; sous la conjecture de Vandiver, il y a égalité. Donc, si $l \leq 125000$, le l-rang de $\mathrm{Cl}(F)$ est égal à s. En fait, pour $l \leq 125000$, la l-partie de $\mathrm{Cl}(F)$ est élémentaire, c'est à dire, isomorphe à $(\mathbf{Z}/l\mathbf{Z})^s$. Par la théorie du corps de classes, cela implique qu'il y a exactement $2^s - 1$ extensions cycliques L de F de degré l et non ramifiées. On a :

Proposition 3.5. *Soit l un nombre premier, $l \leq 125000$, et $F = \mathbf{Q}(\zeta_l)$. Si L est une extension de F de degré l et non ramifiée, alors $\mathfrak{O}_L$ possède une base normale sur $\mathfrak{O}_F$, qu'on peut construire explicitement.*

D'après la remarque 3.3, il suffit de montrer qu'il existe $u \in \mathfrak{O}_L^*$ tel que $u^l \in \mathfrak{O}_F$ et $L = F(u)$. En effet, soit pour chaque $a \in \{0, \ldots, l-1\}$, $\sigma_a \in \mathrm{Gal}(F/\mathbf{Q})$ défini par $\sigma_a(\zeta_l) = \zeta_l^a$ et soit g une racine primitive modulo l. Pour chaque i pair, $2 \leq i \leq l-3$, on définit :

$$E_i = \prod_{a=1}^{l-1} \left(\zeta_l^{(1-g)/2} \, \frac{1 - \zeta_l^g}{1 - \zeta_l} \right)^{a^i \sigma_a^{-1}} . \tag{66}$$

On a $E_i \in \mathfrak{O}_F^*$ pour tout i. De plus, on peut montrer que si $i_1 < \cdots < i_s$ sont les indices d'irrégularité pour l et $l \leq 125000$, alors $F(E_{i_1}^{1/l}, \ldots, E_{i_s}^{1/l})$ est la l-extension abélienne maximale non ramifiée de F ([19], chap. VIII). ∎

4. A propos d'un résultat de F. Kawamoto

Soit l un nombre premier, $a \in \mathbf{Z}$ sans puissance l-ième et satisfaisant la congruence $a^{l-1} \equiv 1 \mod l^2$; soit $F = \mathbf{Q}(\zeta_l)$ et $E = F(a^{1/l})$. F. Kawamoto a montré dans ([9],[10]) que $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$. On va déduire ce théorème des résultats précédents.

Lemme 4.1. *Soit $a \in \mathbf{Z}$ sans puissance l-ième. Alors l'extension*

$$\mathbf{Q}(\zeta_l, a^{1/l})/\mathbf{Q}(\zeta_l)$$

est modérément ramifiée si et seulement si $a^{l-1} \equiv 1 \mod l^2$.

D'après le critère de Hecke (proposition 1.3), il suffit de montrer que $a^{l-1} \equiv 1 \mod l^2$ si et seulement s'il existe $\beta \in F$ tel que $a\beta^l \equiv 1 \mod {}^* (1-\zeta_l)^l$; par le même raisonnement qu'on a fait dans la démonstration de la proposition 2.10, cela est équivalent à l'existence d'un élément $x \in \mathfrak{O}_F$ tel que $a \equiv x^l \mod (1-\zeta_l)^l$.

On a l'égalité $(1-\zeta_l)^l \cap \mathbf{Z} = l^2\mathbf{Z}$. On en déduit un homomorphisme injectif de groupes :

$$(\mathbf{Z}/l^2\mathbf{Z})^* \xrightarrow{\varphi} (\mathfrak{O}_F/(1-\zeta_l)^l\mathfrak{O}_F)^*. \tag{67}$$

Ainsi $a^{l-1} \equiv 1 \mod l^2$ équivaut à $\varphi(a)^{l-1} = 1$. Or on sait que le groupe $(\mathfrak{O}_F/(1-\zeta_l)^l\mathfrak{O}_F)^*$ est produit direct $\mathbf{C}_l^{l-1} \times \mathbf{C}_{l-1}$ (lemme 2.9). On en déduit que $\varphi(a)^{l-1} = 1$ si et seulement si $\varphi(a)$ est une puissance l-ième dans ce groupe. ∎

Proposition 4.2. *(F. Kawamoto) Soit l un nombre premier, a un entier sans puissance l-ième et satisfaisant la congruence $a^{l-1} \equiv 1 \mod l^2$, $F = \mathbf{Q}(\zeta_l)$ et $E = F(a^{1/l})$. Alors $\mathfrak{O}_E$ possède une base normale sur $\mathfrak{O}_F$, qu'on peut déterminer explicitement.*

Du lemme 4.1 on déduit que l'extension E/F est modérément ramifiée. Soit α une racine l-ième de a. Alors $\alpha \in \mathfrak{O}_E$, $\alpha^l \in \mathfrak{O}_F$ et $E = F(\alpha)$. De plus, $v_{\mathfrak{p}}(a\mathfrak{O}_F) < l$ pour tout idéal premier $\mathfrak{p}$ de F, car a est premier avec l et le seul premier qui se ramifie dans $F/\mathbf{Q}$ est l. Grâce à la proposition 2.10, il existe $u \in \mathfrak{O}_F^*$ tel que $\gamma = u\alpha$ est un générateur de Kummer de E sur F tel que $\gamma^l\mathfrak{O}_F = a\mathfrak{O}_F$ et $\gamma \equiv 1 \mod (1-\zeta_l)$.

On écrit $a = \prod_{i=1}^{l-1} a_i^i$, où les a_i sont des entiers premiers entre eux et sans facteur carré; soit $\mathfrak{a}_i = a_i\mathfrak{O}_F$ $(1 \leq i \leq l-1)$. On a $\gamma^l\mathfrak{O}_F = \prod_{i=1}^{l-1} \mathfrak{a}_i^i$ où les $\mathfrak{a}_i$ sont des idéaux entiers de F premiers entre eux et sans facteur carré. Les idéaux $\mathfrak{b}_j$ $(0 \leq j \leq l-1)$ associés aux $\mathfrak{a}_i$ sont principaux; plus précisément, $\mathfrak{b}_j = b_j\mathfrak{O}_F$ avec $b_j \in \mathbf{Z}$ défini par :

$$b_j = \prod_{i=1}^{l-1} a_i^{[ij/l]}, \qquad 0 \leq j \leq l-1. \tag{68}$$

Pour démontrer que γ est un générateur de Kummer de E sur F qui satisfait les conditions exigées dans le théorème 2.1, il suffit de montrer qu'il existe des unités $v_j \in \mathfrak{O}_F^*$ telles que $b_j \equiv v_j \mod l$ $(0 \leq j \leq l-1)$. Or si $x \in \mathbf{Z}$ et si m est le représentant de x modulo l dans $\{1, \ldots, l-1\}$, on a $u_m \equiv m \mod (1-\zeta_l)$ (avec $u_m = (\zeta^m - 1)/(\zeta - 1)$), donc $u_m^l \equiv m \mod l$ et par conséquent $x \equiv u_m^l \mod l$; cela veut dire que l'existence des v_j est assurée. Alors, d'après le théorème 2.1, l'élément :

$$a = (1/l)\sum_{j=0}^{l-1}(\gamma^j v_j / b_j) \tag{69}$$

et ses conjugués constituent une base normale de $\mathfrak{O}_E$ sur $\mathfrak{O}_F$. ∎

Remarque 4.3 Avec les hypothèses de la proposition, on a $E = \mathbf{Q}(\zeta_l, a^{1/l})$; puisque cette extension est modérément ramifiée sur $\mathbf{Q}$ et que son groupe de Galois ne possède pas de représentation symplectique, on sait grâce à la conjecture de Fröhlich démontrée par M. J. Taylor ([17]) que $\mathfrak{O}_E$ possède une base normale sur $\mathbf{Z}$. Mais on sait que cette propriété n'implique pas l'existence d'une base normale de $\mathfrak{O}_E$ sur $\mathbf{Z}[\zeta_l]$.

Bibliographie

[1] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques, dans Collected Papers*, Addison-Wesley, 1965, (réimpression chez Springer Verlag), 229–231.

[2] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Progress in Mathematics **66**, Birkhäuser, Boston, 1987.

[3] A. Fröhlich, *The module structure of Kummer extensions over Dedekind domains*, J. reine angew. Math. **209** (1962), 39–53.

[4] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, J. reine angew. Math. **286/ 287** (1976), 380–440.

[5] A. Fröhlich, *Galois module structure of algebraic integers*, Springer Verlag, 1983.

[6] E. J. Gómez Ayala, *Bases normales d'entiers et multiplication complexe*, thèse, Université Bordeaux I, 1991.

[7] E. J. Gómez Ayala, R. Schertz, *Eine Bemerkung zur Galoismodulstruktur in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, J. Number Theory **44** (1993), 41–46.

[8] E. Hecke, *Lectures on the theory of algebraic numbers*, Springer Verlag, New York, 1981.

[9] F. Kawamoto, *On normal integral bases*, Tokyo J. Math. **7** (1984), 221–231.

[10] F. Kawamoto, *Remark on "On normal integral bases"*, Tokyo J. Math. **8** (1985), 275.

[11] S. Lang, *Algebraic number theory*, Addison-Wesley, 1970.

[12] H. B. Mann, *On integral bases*, Proc. Amer. Math. Soc. **9** (1958), 167–172.

[13] L. R. McCulloh, *A Stickelberger condition on Galois module structure for Kummer extensions of prime degree, dans Algebraic Number Fields*, Proceedings of the Durham Symposium 1975, Academic Press, London 1977, 525–538.

[14] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[15] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1963.

[16] M. J. Taylor, *Galois module structure of rings of integers in Kummer extensions*, Bull. London Math. Soc. **12** (1980), 96–98.

[17] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41–79.

[18] M. J. Taylor (with contributions by N. P. Byott), *Hopf orders and Galois module structure,* dans : *Group Rings and Class Groups*, K. W. Roggenkamp et M. J. Taylor, DMV Seminar, Band 18, Birkhäuser, 1992.

[19] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83**, Springer Verlag, 1982.

E. J. Gómez Ayala
Departamento de Matemáticas
Facultad de Ciencias
Universidad del País Vasco
Apartado 644
48080 Bilbao
España