

REMARQUES SUR L'ARITHMETIQUE DE CERTAINES
EXTENSIONS METACYCLIQUES

Jean COUGNARD

REMARQUES SUR L'ARITHMETIQUE DE CERTAINES

EXTENSIONS METACYCLIQUES

par Jean COUGNARD

Le but de ce travail est d'étudier les anneaux d'entiers d'extensions métacycliques de degré $p^s n$ (p premier, n diviseur de $p-1$) en utilisant les propriétés de groupes de cohomologie associés à ces anneaux d'entiers et les théorèmes de structure de modules sur certains ordres héréditaires. On déduit de ces propriétés que le lien entre les sommes de Gauss galoisiennes et les invariants définis par A. Fröhlich ([5], [6]) dans le cas des extensions modérément ramifiées existe également pour les extensions métacycliques de \mathbb{Q} que nous étudions. Une telle relation était déjà connue pour les extensions abéliennes de \mathbb{Q} ([8]) et nous sommes en mesure de la démontrer également pour les extensions du corps des nombres rationnels dont le groupe de Galois est quaternionien d'ordre 8. Les résultats du § 2 généralisent ceux que nous avons énoncés dans [4] (avec $s = 1$ et n premier). Nous avons tenu à faire figurer cette généralisation car l'introduction de l'opérateur θ due à J.-F. Jaulent ([7]) rend la démonstration du Théorème 2 plus agréable.

§ 1 - NOTATIONS ET RAPPELS.

Dans ce qui suit p désigne un nombre premier impair, t un entier supérieur ou égal à 1 et n un diviseur de $p-1$. On note G_t le groupe engendré par les éléments σ et τ vérifiant les relations :

$$(1) \quad \sigma^{p^t} = \tau^n = 1 \quad \text{et} \quad (2) \quad \tau \sigma \tau^{-1} = \sigma^r$$

où r désigne une racine primitive n -ième de l'unité modulo p^t . Pour tout entier u ($0 \leq u \leq t$) on note H_u le sous-groupe de G_t engendré par $\sigma^{p^{t-u}}$; T est le sous-groupe engendré par τ .

Soit κ un corps et N_t/κ une extension galoisienne de groupe de Galois isomorphe à G_t , on note N_u (resp. K_u) le sous-corps de N_t formé des éléments invariants par H_{t-u} (resp. H_{t-u} et T), l'entier t étant fixé on pose pour $u = t$ (resp. $u = 0$) $N_t = N$ (resp. $N_0 = \kappa$).

Si L est une extension algébrique de degré fini de \mathbb{Q} (resp. d'un complété ℓ -adique \mathbb{Q}_ℓ de \mathbb{Q}), on note O_L la clôture intégrale de \mathbb{Z} (resp. de \mathbb{Z}_ℓ) dans L . Pour rester fidèle aux usages, les extensions cyclotomiques de \mathbb{Q} (resp. de \mathbb{Q}_ℓ) font exception à cette règle : on note ζ_t une racine primitive p^t -ième de l'unité, $\zeta_u = \zeta_t^{p^{t-u}}$ et $\mathbb{Z}[\zeta_u] = O_{\mathbb{Q}}(\zeta_u)$ (resp. $\mathbb{Z}_\ell[\zeta_u] = O_{\mathbb{Q}_\ell}[\zeta_u]$). On choisit un générateur s de $\text{Gal}(\mathbb{Q}(\zeta_t)/\mathbb{Q}) \simeq \text{Gal}(\mathbb{Q}_p(\zeta_t)/\mathbb{Q}_p)$; on en déduit une fonction $v(m)$ de $(\mathbb{Z}/p^t\mathbb{Z})^*$ à valeurs dans $(\mathbb{Z}/p^t\mathbb{Z})^*$ définie par : $s^m(\zeta_t) = \zeta_t^{v(m)}$.

Etant donné un anneau de Dedekind \mathfrak{o} de corps des fractions L et deux \mathfrak{o} -réseaux M, M' d'un L -espace vectoriel V on désigne par $\chi_{\mathfrak{o}}(M, M')$ l'invariant relatif de ces deux réseaux (cf. [11] pour les propriétés de cet invariant et le lien avec les discriminants).

La relation de commutation (2) définit un caractère p -adique μ du groupe

$$T : \quad \tau^i \sigma \tau^{-i} = \sigma^{\mu(\tau^i)}$$

et $\mu_U(\tau^i)$ est l'entier vérifiant : $\mu_U(\tau^i) \equiv \mu(\tau^i) (p^U)$, $0 \leq \mu_U(\tau^i) < p^U$. La congruence $p \equiv 1(n)$ fait que les caractères p -adiques irréductibles de T sont de degré 1 ; ils forment un groupe multiplicatif \hat{T} . Pour chaque $\psi \in \hat{T}$ on note e_ψ l'idempotent de $\mathbb{Q}_p[T]$ associé à ψ .

Soit $\chi = \chi_t$ un caractère fidèle de degré 1 de H_t à valeurs dans \mathbb{C} ; pour tout entier u ($0 \leq u \leq t$) $\chi_{t-u} = \chi^{p^u}$ est trivial sur H_u et la représentation induite $\rho_{t-u} = \text{Ind}_{H_t}^{G_t}(\chi_{t-u})$ est une représentation absolument irréductible de degré n de G_t dont le noyau est H_u . On peut considérer cette représentation comme une représentation fidèle de $G_{t-u} = \text{Gal}(N_{t-u}/\kappa)$. Toute représentation absolument irréductible de degré n de G_{t-u} ($t \neq u$) s'obtient de la même façon en prenant un caractère conjugué de χ_{t-u} , ces représentations ont même con-

ducteur d'Artin. On désigne par c_u le caractère de ρ_u et E_u le sous-corps de \mathbb{C} obtenu en adjoignant à \mathbb{Q} les valeurs de c_u . On a $E_u \subset \mathbb{Q}(\zeta_u)$ et $[\mathbb{Q}(\zeta_u) : E_u] = n$.

Etant donné un anneau de Dedekind \mathfrak{o} de corps des fractions L et M/L une extension galoisienne modérément ramifiée de groupe de Galois Γ , on construit la L algèbre centrale simple A dont les éléments sont les sommes

$\sum_{\gamma \in \Gamma} a_\gamma \gamma$ munie de la multiplication définie par

$$(a_\gamma \gamma) (a_{\gamma'} \gamma') = a_\gamma \gamma (a_{\gamma'} \gamma').$$

Ceux des éléments de A dont les coefficients a_γ appartiennent à O_M constituent un ordre héréditaire $\mathfrak{O}(M/L)$ et tout $\mathfrak{O}(M/L)$ -module sans torsion est une somme directe de sous-modules isomorphes à des idéaux ambiges de M/L . Nous utilisons de tels ordres dans deux cas :

a) L est une extension algébrique finie de \mathbb{Q}_p , on note π une uniformisante de O_M , e l'indice de ramification de M/L ; les idéaux ambiges sont les $\pi^i O_M$ ($0 \leq i < e$). En désignant par Γ' le groupe d'inertie de l'extension M/L , ceux des idéaux $\pi^i O_M$ qui apparaissent dans la décomposition d'un $\mathfrak{O}(M/L)$ -module \mathfrak{R} sont donnés par la structure de $(O_M/\pi O_M)[\Gamma']$ module de $(O_M/\pi O_M) \otimes_{O_M} \mathfrak{R}$ (cf. [10]). En particulier on a $\mathfrak{O}(M/L) \simeq \left[\bigoplus_{i=0}^{e-1} \pi^i O_M \right][\Gamma : \Gamma']$ et on a un isomorphisme de $\mathfrak{O}(M/L)$ -module entre $\pi^i O_M$ et $\pi^{i+e} O_M$ quel que soit i .

b) $L = E_u$, $M = \mathbb{Q}(\zeta_u)$.

Pour plus de précision, on peut consulter [10] ou [12].

§ 2 - EXTENSIONS D'UN CORPS p-ADIQUE.

On suppose dans ce paragraphe que \mathfrak{k} est une extension algébrique de degré fini de \mathbb{Q}_p . Soit I le groupe d'inertie de l'extension N_t/\mathfrak{k} , on sait que G_t/I est cyclique ; le sous-corps de N_t formé des éléments invariants par I est un sous-corps k^I de k , en particulier N_t/k est totalement ramifiée. Les groupes de cohomologie modifiés au sens de Tate $\hat{H}^m(H_t, O_{N_t})$ sont des p -groupes finis sur lesquels le groupe T opère, ce sont donc des $\mathfrak{O}(k/\mathfrak{k})$ -modules et, par restriction, des $\mathbb{Z}_p[T]$ -modules finis. Le foncteur restriction de la catégorie

des $\mathcal{O}(k/\kappa)$ -modules finis dans la catégorie des $\mathbb{Z}_p[T]$ -modules finis induit un homomorphisme entre les groupes de Grothendieck $G_o^t(\mathcal{O}(k/\kappa))$ et $G_o^t(\mathbb{Z}_p[T])$ de ces catégories. On démontre :

Théorème 1 : Les $\mathbb{Z}_p[T]$ -modules $\hat{H}^o(H_t, O_{N_t})$ et $\hat{H}_o(H_t, O_{N_t})$ ont même image dans $G_o^t(\mathbb{Z}_p[T])$.

Ce théorème se déduit du résultat plus précis :

Théorème 2 : Les $\mathcal{O}(k/\kappa)$ -modules $\hat{H}^o(H_t, O_{N_t})$ et $\hat{H}_o(H_t, O_{N_t})$ ont même image dans $G_o^t(\mathcal{O}(k/\kappa))$.

Cette propriété résulte d'une série de Lemmes. Soit $G_o(\mathcal{O}(k/\kappa))$ le groupe de Grothendieck de la catégorie des $\mathcal{O}(k/\kappa)$ -modules de type fini ; si M est un $\mathcal{O}(k/\kappa)$ -module de type fini (resp. fini) on note $[M]$ (resp. (M)) son image dans $G_o(\mathcal{O}(k/\kappa))$ (resp. $G_o^t(\mathcal{O}(k/\kappa))$). L'application qui, à tout $\mathcal{O}(k/\kappa)$ -module fini associe son ordre, définit un homomorphisme du groupe $G_o^t(\mathcal{O}(k/\kappa))$ dans \mathbb{Q}^* noté ord (pour tout anneau A , A^* est le groupe multiplicatif des éléments inversibles de A).

Soit $x \in \kappa^*$, il existe $m \in O_\kappa - \{0\}$ tel que $mx \in O_\kappa$, ceci permet de définir un homomorphisme δ de κ^* dans $G_o^t(\mathcal{O}(k/\kappa))$ par :

$$\delta(x) = \left(\mathcal{O}(k/\kappa) / m \mathcal{O}(k/\kappa) \right) - \left(\mathcal{O}(k/\kappa) / mx \mathcal{O}(k/\kappa) \right).$$

On en déduit la suite exacte :

$$0 \rightarrow O_\kappa^* \rightarrow \kappa^* \xrightarrow{\delta} G_o^t(\mathcal{O}(k/\kappa)) \rightarrow G_o(\mathcal{O}(k/\kappa))$$

qui est un cas particulier de la suite exacte du Théorème 2 de [13]. On a immédiatement le lemme suivant :

Lemme 1 : L'homomorphisme de $G_o^t(\mathcal{O}(k/\kappa))$ dans $G_o^t(\mathcal{O}(k/\kappa)) \times \mathbb{Q}^*$ qui, à (M) associe $([M], \text{ord}((M)))$, est injectif.

Démonstration : cf. [4].

Remarque : Comme $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} O_{N_t}$ est un $\mathbb{Q}_p[H_t]$ -module libre, les $\mathcal{O}(k/\kappa)$ -modules

$\hat{H}^0(H_t, O_{N_t})$ et $\hat{H}_0(H_t, O_{N_t})$ ont même ordre, le théorème 2 équivaut donc à démontrer qu'ils ont même image dans $G_0(\mathcal{O}(k/\kappa))$. Le groupe T opérant sur $O_{N_t}, (1-\sigma)O_{N_t}, O_k$ on a la suite exacte de $\mathcal{O}(k/\kappa)$ -modules :

$$0 \rightarrow \hat{H}_0(H_t, O_{N_t}) \rightarrow \frac{O_{N_t}}{(1-\sigma)O_{N_t}} \xrightarrow{T_{N_t/k}} O_k \rightarrow \hat{H}^0(H_t, O_{N_t}) \rightarrow 0.$$

La démonstration du Théorème 2 se réduit donc à celle de l'égalité :

$$[O_{N_t}/O_k] = [(1-\sigma)O_{N_t}].$$

Lemme 2 : Le $\mathcal{O}(k/\kappa)$ -module O_{N_t}/O_k est isomorphe à $\mathcal{O}(k/\kappa)^{\frac{p^t-1}{n}}$.

Démonstration : Compte tenu des rappels, il suffit de démontrer le lemme lorsque k/κ est totalement ramifiée. Soit alors π (resp. π_t) une uniformisante de k (resp. K_t) ; on peut choisir π de telle sorte que $\tau(\pi) = \epsilon \pi$ où ϵ est une racine

primitive n -ième de l'unité. L'élément $\pi^i = \pi \pi_t^{\frac{p^t-1}{n}}$ est une uniformisante de O_{N_t} et, l'extension N_t/κ étant totalement ramifiée on a un isomorphisme de $\mathcal{O}(k/\kappa)$

modules entre O_{N_t}/O_k et $\bigoplus_{i=1}^{p^n-1} O_k \pi^i$ il suffit alors de constater le $\mathcal{O}(k/\kappa)$ isomorphisme entre $O_k \pi^{i^1}$ et $O_k \pi^i$ et d'utiliser les résultats rappelés au § 1.

Notation : Soit θ l'élément de $\mathbb{Z}_p[H_t]$ égal à $\frac{1}{n} \sum_{i=0}^{n-1} \mu(\tau^{-i}) \sigma^{\mu(\tau^i)}$. L'utilité de cet élément tient au résultat suivant dont on trouvera une démonstration dans [7] (chapitre II Scolie de la prop. II.11).

Lemme 3 : L'idéal d'augmentation $(1-\sigma)\mathbb{Z}_p[H_t]$ de $\mathbb{Z}_p[H_t]$ admet l'élément θ comme générateur ; dans $\mathbb{Z}_p[G_t]$ on a la relation $e_{\psi} \theta = \theta e_{\psi}^{-1}$ pour tout $\psi \in \hat{T}$.

Fin de la démonstration du Théorème 2 : Il suffit de démontrer que les $\mathcal{O}(k/\kappa)$ -modules O_{N_t}/O_k et $(1-\sigma)O_{N_t}$ sont isomorphes, donc, si k^1 est le sous-corps

de k invariant par le groupe d'inertie, que les $(O_k/(\pi))[\text{Gal}(k/k^I)]$ -modules $O_k/(\pi) \otimes_{O_k} (O_{N_t}/O_k)$ et $O_k/(\pi) \otimes_{O_k} (1-\sigma)O_{N_t}$ sont isomorphes.

La multiplication par θ dans O_{N_t} définit un O_k -isomorphisme entre O_{N_t}/O_k et $(1-\sigma)O_{N_t}$ et le nombre de facteurs de $O_k/(\pi) \otimes_{O_k} (1-\sigma)O_{N_t}$ associés à l'idempotent $e_{\psi \mu^{-1}}$ est égal à celui de $O_k/(\pi) \otimes_{O_k} (O_{N_t}/O_k)$ correspondants à l'idempotent e_{ψ} . D'après le lemme 2, pour chaque ψ le nombre de facteurs de $(O_k/(\pi)) \otimes_{O_k} (O_{N_t}/O_k)$ est indépendant de ψ , ce qui achève la démonstration.

Soient u et v deux entiers vérifiant $0 \leq v \leq u \leq t$, le groupe T opère sur les groupes $\hat{H}^o(H_{t-v}/H_{t-u}, O_{N_u})$ et $\hat{H}_o(H_{t-v}/H_{t-u}, O_{N_u})$ en appliquant le théorème 2 à l'extension N_u/K_v , on obtient le :

Corollaire 1 : Les $\mathbb{Z}_p[T]$ -modules $\hat{H}^o(H_{t-v}/H_{t-u}, O_{N_u})$ et $\hat{H}_o(H_{t-v}/H_{t-u}, O_{N_u})$ ont même image dans $G_o^t(\mathbb{Z}_p[T])$.

Soit maintenant l'ordre $\mathfrak{o}(\mathbb{Q}_p(\zeta_t)/E_t) = \Lambda_t$. Il existe un isomorphisme entre les groupes T et $\text{Gal}(\mathbb{Q}_p(\zeta_t)/E_t)$ qui envoie le générateur τ de T sur l'automorphisme défini par $\zeta_t \rightsquigarrow \zeta_t^\tau$ on en déduit un isomorphisme d'algèbres entre $\mathbb{Z}_p[G_t]/(1+\sigma p^{t-1} + \dots + \sigma^{p-1} p^{t-1})$ et Λ_t en donnant ζ_t pour image à σ . On a alors :

Corollaire 2 : Le Λ_t -module $O_{N_t}/O_{N_{t-1}}$ est libre de rang $[\kappa : \mathbb{Q}_p]$.

Démonstration : D'après [10] (prop. 3 et prop. 6) il faut et il suffit que $(O_{N_t}/O_{N_{t-1}})/(1-\sigma)(O_{N_t}/O_{N_{t-1}})$ soit un $\mathbb{F}_p[T]$ -module libre de rang $[\kappa : \mathbb{Q}_p]$. On note \mathcal{C} (resp. \mathcal{C}') la trace dans l'extension N_t/k (resp. N_{t-1}/k) restreinte aux anneaux d'entiers. On a immédiatement la suite exacte :

$$0 \longrightarrow \frac{\ker \mathcal{C}}{(\ker \mathcal{C}') + (1-\sigma)O_{N_T}} \longrightarrow \frac{O_{N_T}}{O_{N_{t-1}} + (1-\sigma)O_{N_T}} \xrightarrow{\mathcal{C}} \frac{\mathcal{C}(O_{N_T})}{p \mathcal{C}'(O_{N_{t-1}})} \longrightarrow 0.$$

Or dans $G_o^t(\mathbb{Z}_p[T])$ nous avons :

$$\left(\frac{\ker \mathcal{C}}{(\ker \mathcal{C}') + (1-\sigma)O_{N_t}} \right) = (\hat{H}_o(H_t, O_{N_t})) - (\hat{H}_o(H_t/H_1, O_{N_{t-1}})).$$

Ce qui, d'après le Théorème 2, est égal à :

$$\begin{aligned} (O_k/\mathcal{C}(O_{N_t})) - (O_k/\mathcal{C}'(O_{N_{t-1}})) &= (O_k/\mathcal{C}(O_{N_t})) - \left(\frac{pO_k}{p\mathcal{C}'(O_{N_{t-1}})} \right) \\ &= (O_k/pO_k) - (\mathcal{C}(O_{N_t})/p\mathcal{C}'(O_{N_t})) \end{aligned}$$

ce qui donne dans $G_o^t(\mathbb{Z}_p[T])$: $\left(\frac{O_{N_t}}{O_{N_{t-1}} + (1-\sigma)O_{N_t}} \right) = (O_k/pO_k) = [\kappa : \mathbb{Q}_p](\mathbb{F}_p[T])$

car l'extension k/κ est modérément ramifiée et O_κ est \mathbb{Z}_p -libre de rang $[\kappa : \mathbb{Q}_p]$; ceci termine la démonstration du Théorème.

§ 3 - PROPRIETES LOCALES D'EXTENSIONS METACYCLIQUES RELATIVES DE \mathbb{Q} .

Dans ce paragraphe, κ est une extension algébrique de degré fini de \mathbb{Q} . Pour toute place \mathcal{L} d'une extension L de \mathbb{Q} de degré fini, on note $L_{\mathcal{L}}$ (resp. $O_{L_{\mathcal{L}}}$) son complété (resp. le complété de la clôture intégrale de \mathbb{Z}) en \mathcal{L} .

Fixons u ($0 \leq u \leq t$), notons \mathfrak{p} les idéaux premiers au-dessus de p dans κ , $\mathfrak{p}_i^!$ ceux au-dessus de \mathfrak{p} dans N_u , $\mathfrak{p}_{i,j}$ ceux de N_t au-dessus de $\mathfrak{p}_i^!$. Soit $D_{i,j}$ le groupe de décomposition de $\mathfrak{p}_{i,j}$ dans N_t/κ puis $V_{i,j}^u = H_{t-u} \cap D_{i,j}$ et $T_{i,j} = T \cap D_{i,j}$.

Proposition 1 : Les groupes $\hat{H}_o(H_{t-u}, O_{N_t})$ et $\hat{H}^o(H_{t-u}, O_{N_t})$ ont même image dans $G_o^t(\mathbb{Z}_p[T])$.

Démonstration : Pour tout entier m , le groupe $\hat{H}^m(H_{t-u}, O_{N_t})$ est un p -groupe fini, donc isomorphe à $\mathbb{Z}_p \otimes_{\mathbb{Z}} \hat{H}^m(H_{t-u}, O_{N_t})$ c'est-à-dire à

$\hat{H}^m(H_{t-u}, \mathbb{Z}_p \otimes_{\mathbb{Z}} O_{N_t})$ qui peut s'écrire $\hat{H}^m(H_{t-u}, \prod_{\mathfrak{p}_{i,j}} O_{N_{\mathfrak{p}_{i,j}}})$. Ce dernier groupe est lui-même isomorphe à

$$\prod_{\mathfrak{p}_i | p} \hat{H}^m(H_{t-u}, \prod_j O_{N_{\mathfrak{p}_{i,j}}})$$

pour chaque indice i fixons $\mathfrak{p}_i = \mathfrak{p}_{i,0}$ une des places $\mathfrak{p}_{i,j}$ au-dessus de \mathfrak{p}_i , on a $\prod_j O_{N_{\mathfrak{p}_{i,j}}} \simeq \mathbb{Z}_p[H_{t-u}] \otimes_{\mathbb{Z}_p[V_{i,j}^u]} O_{N_{\mathfrak{p}_i}}$, ce qui d'après le lemme de Shapiro donne

$$\hat{H}^m(H_{t-u}, O_{N_t}) \simeq \prod_{\mathfrak{p}_i | p} \hat{H}^m(V_{i,0}^u, O_{N_{\mathfrak{p}_i}}). \text{ Posons } T_i = T_{i,0}, \text{ le groupe } T \text{ opère sur}$$

$$\prod_{\mathfrak{p}_i | p} \hat{H}^m(V_{i,0}^u, O_{N_{\mathfrak{p}_i}}). \text{ Soit } \Gamma_o^m \text{ l'un des groupes } \hat{H}^m(V_{i,0}^u, O_{N_{\mathfrak{p}_i}}), T_o \text{ son}$$

stabilisateur dans T et $\Gamma^m = \prod_{\mathfrak{z} \in T/T_o} h_{\Gamma_o^m}$, on a $\Gamma^m = \mathbb{Z}_p[T] \otimes_{\mathbb{Z}_p[T_o]} \Gamma_o^m$.

Il suffit alors d'appliquer le Théorème 2 aux groupes Γ_o^m et de remarquer que l'extension des scalaires de $\mathbb{Z}_p[T_o]$ à $\mathbb{Z}_p[T]$ définit un homomorphisme de $G_o^t(\mathbb{Z}_p[T_o])$ dans $G_o^t(\mathbb{Z}_p[T])$.

Théorème 3 : Le $\mathbb{Z}[G_t]$ -module $O_{N_t}/O_{N_{t-1}}$ est un module localement libre de

$$\text{rang } [\kappa : \mathbb{Q}] \text{ sur } \frac{\mathbb{Z}[G]}{(1 + \sigma^{p^t-1} + \dots + \sigma^{(p-1)p^t-1})}$$

Démonstration : L'ordre $\mathbb{Z}[G_t]/(1 + \sigma^{p^t-1} + \dots + \sigma^{(p-1)p^t-1})$ est isomorphe à $\mathcal{O}(\mathbb{Q}(\zeta_t)/E_t)$ compte tenu des isomorphismes entre H_t et le groupe des racines p^t -èmes de l'unité d'une part et entre les groupes T et $\text{Gal}(\mathbb{Q}(\zeta_t)/E_t)$ d'autre part. Puisque p est le seul idéal ramifié dans $\mathbb{Q}(\zeta_t)/E_t$, il faut et il suffit que

$\mathbb{Z}_p \otimes_{\mathbb{Z}} O_{N_t}/O_{N_{t-1}}$ soit libre de rang $[\kappa : \mathbb{Q}]$ sur $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}(\mathbb{Q}(\zeta_t)/E_t)$; donc que

$O_{N_t}/O_{N_{t-1}} + (1-\sigma)O_{N_t}$ soit $\mathbb{F}_p[T]$ -libre de rang $[\kappa : \mathbb{Q}]$. La démonstration est

analogue à celle du corollaire 1 au Théorème 2.

Remarques : Lorsque n est premier et $\kappa = \mathbb{Q}$, il résulte des calculs de [2] (chapitre IX) que $O_{N_t}/O_{N_{t-1}}$ est libre de rang 1 sur $\mathbb{Q}(\zeta_t)/E_t$. Le même résultat est démontré dans [7] (chapitre III) en supposant n quelconque mais $\mathbb{Q}(\zeta_t)$ et N_t linéairement disjointes sur \mathbb{Q} . Une démonstration complète (n quelconque, et pas d'hypothèse de disjonction linéaire) sera fournie dans la version définitive de ce travail.

§ 4 - LIEN AVEC LES SOMMES DE GAUSS GALOISIENNES.

Dans ce paragraphe, on suppose que $\kappa = \mathbb{Q}$; pour toute représentation ρ de G_t et tout élément x de N_t l'élément $\det \left(\sum_{g \in G_t} g(x) \rho(g-1) \right)$ ne dépend que du caractère c_ρ de ρ on le note $\langle a, c_\rho \rangle_{N/\mathbb{Q}}$.

On désigne par $\tau(c_\rho)$ la somme de Gauss galoisienne associée au caractère c_ρ (cf. [9]). L'action du groupe de Galois de la clôture algébrique de \mathbb{Q} montre que l'élément $\langle a, c_\rho \rangle_{N/\mathbb{Q}} \tau(c_\rho)^{-1}$ appartient au corps $\mathbb{Q}(c_\rho)$ ([5] prop. 1. 5 et Th. 3). Lorsque a parcourt O_N les éléments $\langle a, c_\rho \rangle_{N/\mathbb{Q}} \tau(c_\rho)^{-1}$ engendrent un idéal de $\mathbb{Q}(c_\rho)$ noté $\langle O_N, c_\rho \rangle \tau(c_\rho)^{-1}$. Il est bien connu que si N/\mathbb{Q} est modérément ramifiée, cet idéal est égal à $O_{\mathbb{Q}(c_\rho)}$. Nous nous proposons de démontrer un résultat analogue lorsque l'extension N/\mathbb{Q} est sauvagement ramifiée et que la représentation ρ est une représentation fidèle de G_t ; nous donnons la démonstration lorsque N_t/\mathbb{Q} et $\mathbb{Q}(\zeta_t)$ sont linéairement disjointes sur \mathbb{Q} .

Nous pouvons déjà remarquer, d'après le théorème 4 de [5] que pour les idéaux premiers à np , la valuation de $\langle O_N, c_\rho \rangle \tau(c_\rho)^{-1}$ est nulle.

Pour u fixé, on choisit la représentation matricielle suivante de ρ_u :

$$\rho_u(\sigma) = (\alpha_{i,j}(\sigma)) \quad \text{où} \quad \alpha_{i,j}(\sigma) = \delta_{i,j} \mathbb{G}_u^{r_{n-i}}$$

$$\rho_u(\tau) = (\alpha_{i,j}(\tau)) \quad \text{où} \quad \alpha_{i,j}(\tau) = \delta_{i,j+1}$$

où i (resp. j) l'indice des lignes (resp. des colonnes) est numéroté de 0 à $n-1$ modulo n ; par conséquent :

$$(\alpha_{i,j}(\tau^\ell \sigma^m)) = \rho_U(\tau^\ell \sigma^m) = \delta_{i,j+\ell} \zeta_U^{mr^{n-j}} \text{ ou } \alpha_{i,j}(\tau^\ell \sigma^m) = \delta_{i,j+\ell} \zeta_U^{mr^{n-j}}$$

ce qui donne :

$$\sum_{g \in G_t} g(x) \rho_U(g^{-1}) = \sum_{\ell, m} \sigma^{-m} \tau^{-\ell}(x) \rho_U(\tau^\ell \sigma^m)$$

est une matrice à n lignes, n colonnes dont le coefficient d'indice (i, j) :

$$\sum_m \sigma^{-m} \tau^{j-1}(x) \zeta_U^{mr^{n-j}}$$

on reconnaît là l'expression d'une résolvante de Lagrange ; nous notons pour tout u (0 ≤ u ≤ t), tout x appartenant à N_u et tout caractère ψ de degré 1 de H_t, trivial sur H_{t-u} :

$$\langle x, \psi \rangle_u = \sum_{h \in H/H_{t-u}} h(x) \psi(h^{-1})$$

avec cette notation, le coefficient d'indice (i, j) de la matrice $\sum_{g \in G_t} g(x) \rho_U(g^{-1})$ est donc $\langle \tau^{j-i}(x), \chi_U^{r^{n-j}} \rangle_t$.

Soit S (resp. S') la partie multiplicative de Z formée des éléments premiers à n (resp. à np) ; pour tout Z-module M, on note S⁻¹M (resp. S'^{-1}M) les localisés correspondants.

Choisissons un élément θ_t de O_{N_t} qui engendre avec ses conjugués une base de N_t/Q, l'extension N_t/k étant modérément ramifiée pour les diviseurs de n on suppose de plus que θ_t engendre une base normale de S⁻¹O_{N_t} comme S⁻¹O_k[H_t]-module. Pour 0 ≤ u ≤ t, on pose θ_u = T_{N_t/N_u}(θ_t), cet élément est un générateur de N_u (resp. O_{N_u}) comme Q[G_t/H_{t-u}] (resp. S⁻¹O_k[H_t/H_{t-u}]) module. On peut alors construire une famille f_u (0 ≤ u ≤ t) de k-homomorphismes d'espaces vectoriels définis sur N_u et à valeurs dans k(ζ_u) par :

$$f_u(x) = \frac{\langle x, \chi_u \rangle_u}{\langle \theta_u, \chi_u \rangle_u}.$$

L'image de O_{N_u} par f_u est un réseau pour les anneaux O_k et Z[ζ_u] et que f_u(O_{N_u})

est isomorphe à $O_{N_u}/O_{N_{u-1}}$ ([3] proposition II. 2 et II. 8). On sait aussi que

$O_{N_u}/O_{N_{u-1}}$ est un $\mathfrak{o}(Q(\zeta_u)/E_u)$ module localement libre, donc

$S^{-1}O_{N_u}/S^{-1}O_{N_{u-1}}$ est un $S^{-1}\mathfrak{o}(Q(\zeta_u)/E_u)$ -module libre, soit a_u un généra-

teur. L'image $S^{-1}f(O_{N_u})$ est donc le $S^{-1}Z[\zeta_u]$ réseau engendré par les

éléments $\frac{\langle \tau^{-i} a_u, x_u \rangle_u}{\langle \theta_u, x_u \rangle_u}$ et le discriminant de ce réseau est égal au carré du

déterminant de la matrice $(a_{i,j})$ ($0 \leq i, j \leq n-1$) où

$$a_{i,j} = \tau^j \left(\frac{\langle \tau^{-i} a_u, x_u \rangle_u}{\langle \theta_u, x_u \rangle_u} \right) = \frac{\langle \tau^{j-i} a_u, x_u^{r^{n-j}} \rangle_u}{\langle \tau^j \theta_u, x_u^{r^{n-j}} \rangle_u}.$$

Pour un anneau de Dedekind \mathfrak{o} de corps des fractions L et M/L une extension séparable de degré fini m on note $\Delta_{\mathfrak{o}}(R)$ le discriminant d'un \mathfrak{o} réseau de M , de rang m , relativement à la forme bilinéaire déduite de la trace ([11] ch. IV). On a :

$$(1) \quad S^{-1} \Delta_{Z[\zeta_u]}(f_u(O_{N_u})) = \left(\frac{\langle a_u, \rho_u \rangle_{N_u/Q}}{\prod_{j=0}^{n-1} \langle \tau^j \theta_u, x_u^{r^{n-j}} \rangle_u} \right)^2.$$

On a remarqué que $S^{-1}O_{N_u} = S^{-1}O_k[H_t/H_{t-u}] \cdot \theta_u$, donc

$S^{-1}f_u(O_{N_u}) = S^{-1}O_k[\zeta_u] = S^{-1}O_k[\zeta_u]$ puisque les diviseurs premiers de n

ne sont pas ramifiés dans $k(\zeta_u)/k$, on en déduit :

$$S^{-1} \Delta_{Z[\zeta_u]}(f_u(O_{N_u})) = S^{-1} \Delta_Z(O_k)$$

ce qui donne la relation :

$$S^{-1}(\Delta_Z(O_k)Z[\zeta_u]) = \left(\frac{\langle a_u, \rho_u \rangle_{N_u/K}}{\prod_{j=0}^{n-1} \langle \tau^j \theta_u, x_u^{r^{n-j}} \rangle_u} \right)^2.$$

Si un idéal premier ℓ divisant n n'est pas ramifié dans N_U/k , le choix de θ_U fait que $\prod_{j=0}^{n-1} \langle \tau^j \theta_U, \chi_U^{n-j} \rangle$ est premier à cet idéal or il existe une unité ϵ telle que $\Delta_{\mathbb{Z}}(O_K) = \left(\frac{\tau(\rho_U)}{\tau(\chi_U)} \epsilon \right)^2$, comme $\tau(\chi_U)$ est premier à ℓ , on en déduit que : $\langle a_U, \rho_U \rangle_{N_U/\mathbb{Q}} \tau(\rho_U)^{-1}$ est premier à ℓ et par conséquent que $\langle O_{N_U}, \rho_U \rangle_{N_U/\mathbb{Q}} \tau(\rho_U)^{-1}$ est premier à ℓ . Si par contre l'idéal premier ℓ divisant n est ramifié dans N_U/k il ne peut l'être dans k/\mathbb{Q} et par conséquent l'extension N_U/\mathbb{Q} est modérément ramifiée en ℓ , $\langle O_{N_U}, \rho_U \rangle_{N_U/\mathbb{Q}} \tau(\rho_U)^{-1}$ est égal à $O_{\mathbb{Q}(\rho_U)}$ d'après le Théorème 4 de [5].

Il nous reste à démontrer que la valuation de l'idéal $\langle O_{N_U}, \rho_U \rangle_{N_U/\mathbb{Q}} \tau(\rho_U)^{-1}$ est nulle pour la place de E_U au-dessus de p . Ce résultat va se déduire du calcul de la p -composante du discriminant de N_t/k .

L'anneau $S^{t-1}O_K$ étant principal, le $S^{t-1}O_K$ -module $S^{t-1}O_{N_U}$ est libre. Choisissons une base de $S^{t-1}O_{N_t}$ de la façon suivante : ses éléments sont notés $v_{i,j}$, les indices i, j vérifiant : $0 \leq i \leq t$, pour $i = 0$, $j = 0$ et pour $1 \leq i \leq t$ $0 \leq j \leq \varphi(p^i) - 1$ et les éléments $v_{i,j}$ vérifiant $v_{0,0} = 1$ et pour $i \geq 1$ les $v_{i,j}$ forment une $S^{t-1}O_K$ base de $S^{t-1}(O_{N_i}/O_{N_{i-1}})$.

Soient alors les matrices $B = (b_{i,j})$ et $C = (c_{e,f})$ définies par $0 \leq i, j, e, f \leq p^t - 1$; $b_{0,j} = c_{\ell,0} = 1$ et pour $p^{\ell-1} \leq i, f < p^\ell$ $b_{i,j} = \sigma^j(v_{\ell, i-p^{\ell-1}})$; $c_{e,f} = \chi(\sigma^{-e})^{v(f-p^{\ell-1})}$. Il est bien connu que le produit des carrés des déterminants de B et C vaut $p^{tp^t} \times S^{t-1} \Delta_{O_K}(O_{N_t})$. Si par ailleurs on effectue le produit des deux matrices, on obtient une matrice $D = (d_{i,j})$ dont les coefficients valent :

$$d_{i,0} = T_{N_t/k}(b_{i,0}) ; d_{0,j} = 0 \text{ si } j > 0$$

pour $0 < u \leq t$; $p^{u-1} \leq j < p^u$ $d_{i,j} = \langle b_{i,o}, \chi_u^{v(j-p^{u-1})} \rangle_t$ remarquons que pour $p^{u-1} \leq j < p^u$ et $i < p^{u-1}$ l'élément $b_{i,o}$ appartient à $O_{N_{u-1}}$ et par conséquent $\langle b_{i,o}, \chi_u^{v(j-p^{u-1})} \rangle_t = 0$. On en déduit que le calcul du déterminant de D ne fait intervenir que les déterminants des matrices $(d_{i,j})$ avec i, j vérifiant simultanément soit $i = j = 0$, soit $p^{u-1} \leq i, j < p^u$ auquel cas on a :

$$\begin{aligned} d_{o,o} &= p^t ; d_{i,j} = \langle v_{u, i-p^{u-1}}, \chi_u^{v(j-p^{u-1})} \rangle_t \\ &= p^{t-u} \langle v_{u, i-p^{u-1}}, \chi_u^{v(j-p^{u-1})} \rangle_u = p^{t-u} s^{j-p^{u-1}} (\langle v_{u, i-p^{u-1}}, \chi_u \rangle_u) \end{aligned}$$

cette dernière égalité provenant de la disjonction linéaire entre k et $\mathbb{Q}(\zeta_t)$. On obtient donc, compte tenu de la définition de l'application f_u :

$$d_{i,j} = p^{t-u} s^{j-p^{u-1}} (f_u(v_{u, i-p^{u-1}})) s^{j-p^{u-1}} (\langle \theta_u, \chi_u \rangle_u).$$

Le déterminant de la matrice $(d_{i,j})$ extraite de D avec $p^{u-1} \leq i, j < p^u$ est donc égal à $p^{(t-u)\varphi(p^u)} N_{N_u(\zeta_u)}/N_u (\langle \theta_u, \chi_u \rangle_u) \Delta_{S^{-1}O_k} (S^{-1}f_u(O_{N_u}))$ ce qui conduit à l'égalité :

$$\begin{aligned} p^t p^t S^{-1} \Delta_{O_k} (O_{N_t}) &= p^{2t} \prod_{u=1}^t p^{2(t-u)\varphi(p^u)} N_{N_u(\zeta_u)}/N_u \\ &\quad (\langle \theta_u, \chi_u \rangle_u^2) S^{-1} \Delta_{O_k} (f_u(O_{N_u})) \end{aligned}$$

les deux membres de l'égalité étant dans k , on obtient en prenant la norme dans l'extension k/\mathbb{Q} :

$$\begin{aligned} p^{nt} N_{k/\mathbb{Q}} (S^{-1} \Delta_{O_k} (O_{N_t})) &= p^{2nt} \prod_{u=1}^t p^{2n(t-u)\varphi(p^u)} N_{k/\mathbb{Q}} \\ &\quad (N_{N_u(\zeta_u)}/N_u (\langle \theta_u, \chi_u \rangle_u^2)) N_{k/\mathbb{Q}} (S^{-1} \Delta_{O_k} (f_u(O_{N_u}))) \end{aligned}$$

soit, puisque $\Delta_{O_k} (f_u(O_{N_u})) = \Delta_{O_k} (O_k(\zeta_u)) \chi_{O_k} (O_k(\zeta_u), f_u(O_{N_u}))^2$ et que

$$\chi_Z = N_{k/\mathbb{Q}} \circ \chi_{O_k} :$$

$$p^{ntp^t} N_{k/Q} (S'^{-1} \Delta_{O_k} (O_{N_t})) = p^{2nt} \prod_{u=1}^t p^{2n(t-u)\varphi(p^u)} N_{k/Q}$$

$$\left(N_{N_u(\zeta_u)} / N_u (\langle \theta_u, x_u \rangle_u^2) \right) N_{k/Q} (S'^{-1} \Delta_k (O_k(\zeta_u))) \times \chi_Z^2 (O_k(\zeta_u), f_u(O_{N_u})).$$

En multipliant les deux membres par $\Delta_Z (S'^{-1} O_k) p^{t-1} = \Delta_Z (S'^{-1} O_k)_{u=1}^t \varphi(p^u)$

les relations classiques sur les discriminants nous donnent :

$$p^{ntp^t} \Delta_Z (S'^{-1} O_{N_t}) \Delta_Z^{-1} (S'^{-1} O_k) = p^{2nt} \prod_{u=1}^t p^{2n(t-u)\varphi(p^u)} N_{k/Q}$$

$$\left(N_{N_u(\zeta_u)} / N_u (\langle \theta_u, x_u \rangle_u^2) \right) \Delta_Z (f_u(O_{N_u}))$$

c'est-à-dire :

$$\prod_{u=1}^t \Delta_Z (f_u(S'^{-1} O_{N_u})) = p^{ntp^t - 2nt - \sum_{u=1}^t 2n(t-u)\varphi(p^u)} \Delta_{S'^{-1}Z} (S'^{-1} O_{N_t})$$

$$\Delta_{S'^{-1}Z} (S'^{-1} O_k)^{-1} \prod_{u=1}^t N_{k/Q} \left(N_{N_u(\zeta_u)} / N_u (\langle \theta_u, x_u \rangle_u^{-2}) \right).$$

Si on calcule différemment le membre de gauche, on obtient :

$$\Delta_Z (f_u(S'^{-1} O_{N_u})) = \Delta_Z (S'^{-1} Z[\zeta_u])^n N_{Q(\zeta_u)/Q} \left(\Delta_{S'^{-1}Z[\zeta_u]} (S'^{-1} f_u(O_{N_u})) \right).$$

Ceci donne en remplaçant $S'^{-1} \Delta_Z[\zeta_u] (f_u(O_{N_u}))$ par son expression (1) :

$$\prod_{u=1}^t S'^{-1} \Delta_Z (f_u(O_{N_u})) = \prod_{u=1}^t S'^{-1} (\Delta_Z(Z[\zeta_u])^n) N_{Q(\zeta_u)/Q} \left(\left(\frac{\langle a_u, \rho_u \rangle_{N_u/Q}}{\prod_{j=0}^{n-1} \langle \tau^j \theta_u, x_u^{r^{n-j}} \rangle_u} \right)^2 \right).$$

Si on compare maintenant les deux expressions de $\prod_{u=1}^t S'^{-1} \Delta_Z f_u(O_{N_u})$ on obtient :

$$\prod_{u=1}^t N_{Q(\zeta_u)/Q} \left(\left(\frac{\langle a_u, \rho_u \rangle_{N_u/Q}}{\prod_{j=0}^{n-1} \langle \tau^j \theta_u, x_u^{r^{n-j}} \rangle_u} \right)^2 \right) = \prod_{u=1}^t S'^{-1} \Delta_Z (Z[\zeta_u])^n$$

$$p^{ntp^t - 2nt - \sum_{u=1}^t 2n(t-u)\varphi(p^u)} \varphi(p^u) f(p^u) \times N_{k/Q} \left(N_{N_u(\zeta_u)} / N (\langle \theta_u, x_u \rangle_u^2) \right)$$

où $f(p^u)$ est le conducteur d'Artin du caractère ρ_u .

en remplaçant $\Delta_Z(\mathbb{Z}[\zeta_u])$ par sa valeur, le membre de droite devient :

$$= \prod_{u=1}^t f(\rho_u)^{\varphi(u)} N_{K/\mathbb{Q}} \left(N_{N_u(\zeta_u)/N} \left(\langle \theta_u, x_u \rangle^2 \right) \right)$$

L'action du groupe de Galois de $N(\zeta_u)/\mathbb{Q}(\zeta_u)$ sur le produit :

$$\prod_{j=0}^{n-1} \langle \tau^j \theta_u, x_u \rangle^{n-j}$$

montre que ce dernier appartient à $\mathbb{Q}(\zeta_u)$, on en déduit qu'il en est de même pour $\langle a_u, \rho_u \rangle_{N_u/\mathbb{Q}}^2$ et donc en simplifiant :

$$\prod_{u=1}^t N_{\mathbb{Q}(\zeta_u)/\mathbb{Q}} \left(\langle a_u, \rho_u \rangle_{N_u/\mathbb{Q}}^2 \right) = \prod_{u=1}^t f(\rho_u)^{\varphi(\rho_u)}$$

comme le conducteur d'Artin est dans \mathbb{Q} ceci devient :

$$\prod_{u=1}^t N_{\mathbb{Q}(\zeta_u)/\mathbb{Q}} \left(\langle a_u, \rho_u \rangle_{N_u/\mathbb{Q}}^2 f^{-1}(\rho_u) \right) = 1.$$

Le résultat souhaité se déduit alors du lien entre les sommes de Gauss galoisiennes et le conducteur d'Artin ([9]).

- [1] A. M. BERGE - Anneaux d'Entiers et Ordres Associés - Thèse -
Bordeaux 1979
- [2] J. Y. COUGNARD - Propriétés Galoisiennes des Anneaux d'Entiers -
Thèse - Bordeaux 1975
- [3] J. Y. COUGNARD - Propriétés galoisiennes des anneaux d'entiers des
 p -extensions - Compositio. Mathematica vol. 33 fas. 3 1976
pag. 303-336
- [4] J. Y. COUGNARD - Une propriété de l'anneau des entiers des extensions
galoisiennes non abéliennes de degré pq des rationnels -
à paraître dans Compositio Mathematica
- [5] A. FRÖHLICH - Arithmetic and Galois-module Structure for Tame
extensions - Journal für die reine und angewandte Mathematic
vol. 286-287 1976 p. 380-440
- [6] A. FRÖHLICH - Galois Module Structure - dans Algebraic Number Fields -
pag. 133-191 - Academic Press 1977
- [7] J. -F. JAULENT - Structures galoisiennes dans les extensions métabé-
liennes - Thèse de troisième cycle - Besançon 1979
- [8] H. W. LEOPOLDT - Über die Hauptordnung der ganzen Elementen eines
abelschen Zahlkörpers - Jour. reine angew. Math. 201 (1959)
pag. 119-149
- [9] J. MARTINET - Character Theory and Artin L-functions dans Algebraic
Number Fields - Academic Press 1977 pag. 1-87
- [10] M. ROSEN - Representations of Twisted Group Rings - - Ph. D.
Thesis Princeton 1963
- [11] J. -P. SERRE - Corps locaux - Seconde édition (1968) Hermann

- [12] S. M. J. WILSON - Twisted Group rings and Ramification - Proc. London Math. Soc. (3) 31 (1975) pag. 311-330
- [13] S. M. J. WILSON - Reduced Norms in the K-Theory of Orders - Journal of Algebra 46 (1977) pag. 1-11.