Journal de Théorie des Nombres
de Bordeaux **14** (2002), 1–17

Bases normales relatives en caractéristique positive

par Bruno ANGLÈS

Résumé. Dans cet article, nous étudions la structure galoisienne des anneaux d'entiers des corps de fonctions cyclotomiques dans le cas modéré. Nous montrons qu'en général, si le corps de base est de genre plus grand que 1, ces anneaux ne sont pas libres sur les anneaux de groupes considérés.

Abstract. In this paper, we study the Galois module structure of the ring of integers of cyclotomic function fields in the tame case. We show that, in general, these rings are not free over the group ring if the genus of the base field is greater than 1.

Soient p et ℓ deux nombres premiers impairs avec $p \equiv 1 \pmod{\ell}$. Soit k le sous-corps de $\mathbb{Q}(\zeta_p)$ tel que $[\mathbb{Q}(\zeta_p) : k] = \ell$. Jan Brinkhuis et Jean Cougnard ont montré que $\mathbb{Z}[\zeta_p]$ n'est pas un $O_k[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/k)]$-module libre (voir [3] et [5]). Ce résultat, récemment généralisé par Cougnard ([6]), répond ainsi à un problème posé par Albrecht Fröhlich (voir [7], chapitre VI, paragraphe 1). Dans cet article, nous étudions le problème de Fröhlich pour les corps de fonctions cyclotomiques (voir Théorèmes 3.5 et 4.6).

Soit k le sous-corps quadratique de $\mathbb{Q}(\zeta_p)$. Dans [9], Cornelius Greither propose le problème suivant : soit $\mathcal{M}$ l'ordre maximal de $k[\mathrm{Gal(K/k)}]$, $\mathcal{M}\mathbb{Z}[\zeta_p]$ est-il un $\mathcal{M}$-module libre ? Ce problème reste ouvert. Nous résolvons le problème de Greither pour les corps de fonctions : soit P un polynôme irréductible de degré d, $P \in \mathbb{F}_q[T]$, soit K le P-ième corps de fonctions cyclotomiques et k son sous-corps quadratique (q impair), alors O_K est un $O_k[\mathrm{Gal}(K/k)]$-module libre si et seulement si $d \leq 2$ (voir paragraphe 5), où O_K (respectivement O_k) est la fermeture intégrale de $\mathbb{F}_q[T]$ dans K (respectivement k) ; notons que $O_k[\mathrm{Gal}(K/k)]$ est l'ordre maximal de $k[\mathrm{Gal}(K/k)]$.

Finalement, notons que Cornelius Greither, Daniel R. Replogle, Karl Rubin et Anupam Srivastav ont montré le résultat remarquable suivant : $\mathbb{Q}$ est le seul corps de nombres de type Hilbert-Speiser ([10], Theorem 2).

Manuscrit reçu le 14 avril 2001.

Il serait intéressant de trouver un analogue de ce résultat pour les corps de fonctions sur les corps finis.

1. Notations

Soit $\mathbb{F}_q$ un corps fini ayant q éléments et de caractéristique p. Soit T une indéterminée sur $\mathbb{F}_q$, on pose $Z = \mathbb{F}_q[T]$ et $Q = \mathbb{F}_q(T)$. Soit $\bar{Q}$ une clôture algébrique fixée de Q. Toutes les extensions finies de Q considérées dans cet article sont contenues dans $\bar{Q}$.

Soit L/Q une extension finie. On note :
- O_L : la fermeture intégrale de Z dans L ;
- E_L : le groupe des éléments inversibles de O_L ;
- I_L : le groupe des idéaux fractionnaires non nuls de O_L ;
- P_L : le groupe des idéaux fractionnaires principaux non nuls de O_L ;
- $h(L)$: le cardinal de I_L/P_L ;
- S_L : l'ensemble des places de L au dessus de $1/T$.

Pour tout entier $n \geq 1$, on note $L(n)$ le compositum de L et de $\mathbb{F}_{q^n}$ dans $\bar{Q}$, où $\mathbb{F}_{q^n} \subset \bar{Q}$ est le corps fini ayant q^n éléments.

Soit $Z \to \mathrm{End}_{\mathbb{F}_q}\mathbb{G}_a$, $A \mapsto [A]$, le module de Carlitz (Voir [8], chapitre 3). Soit $P \in Z$ un polynôme irréductible unitaire de degré d. Notons Λ_P l'ensemble des points de P-torsion du module de Carlitz. Fixons $\lambda_P \in \Lambda_P \setminus \{0\}$. On rappelle que le P-ième corps de fonctions cyclotomiques est :

$$K = Q(\Lambda_P) = Q(\lambda_P).$$

Nous renvoyons le lecteur à [11] et [8], chapitre 7, pour les propriétés classiques des corps de fonctions cyclotomiques. Rappelons que :

$$O_K = Z[\lambda_P],$$

et que K/Q une une extension cyclique de degré $q^d - 1$ ramifiée en P et $1/T$, totalement ramifiée en P, le groupe de décomposition de $1/T$ dans K/Q étant isomorphe au groupe d'inertie de $1/T$ qui est isomorphe à $\mathbb{F}_q^*$. Notons $G = \mathrm{Gal}(K/Q)$. Pour $A \in Z \setminus PZ$, on note σ_A l'élément de G tel que :

$$\sigma_A(\lambda_P) = [A](\lambda_P).$$

Fixons $\omega \in \mathbb{F}_{q^d}$ une racine de P. On considère le caractère de Teichmüller $\theta : G \to \mathbb{F}_{q^d}^*$ donné par :

$$\theta(\sigma_A) = A(\omega).$$

Pour tout groupe abélien fini H d'ordre premier à p, on pose :

$$\widehat{H} = \mathrm{Hom}(\mathrm{H}, \bar{\mathrm{Q}}^*).$$

Soient $n, m \in \mathbb{Z}$, $n \geq 1$. On désigne par $[m]_n$ le plus petit entier $k \geq 0$ tel que $k \equiv m \pmod n$. On note (n,m) le plus grand commun diviseur de n et de m.

2. Sommes de Gauss-Thakur généralisées

Dans ce paragraphe, nous généralisons les sommes de Gauss-Thakur définies dans [13] et donnons les principales propriétés de ces sommes. Notons que ces sommes sont identiques à celles introduites par David Goss (voir [8], chapitre 9) excepté le cas particulier du caractère trivial. Nous montrons alors comment on peut construire des bases normales entières à l'aide des ces sommes.

Nous allons travailler dans $K(d) = K(\mathbb{F}_{q^d})$, où $d = \deg P$. Notons $\mathcal{U}$ l'unique premier de $K(d)$ au dessus de $T - \omega$. Notons $F \in \mathrm{Gal}(K(d)/Q)$ le Frobenius, i.e. F est l' identité sur K et pour tout $\zeta \in \mathbb{F}_{q^d}$, $F(\zeta) = \zeta^q$. On identifie G à $\mathrm{Gal}(K(d)/Q(d))$. Pour $A \in Z \setminus PZ$, on note σ_A l'élément de $\mathrm{Gal}(K(d)/Q)$ qui est l'identité sur $Q(d)$ et tel que $\sigma_A(\lambda_P) = [A](\lambda_P)$. On a donc :

$$\mathrm{Gal}(K(d)/Q) = < F > \times G\,.$$

Soit $\chi \in \widehat{G}$, alors $\chi = \theta^i$ pour un $i \in \mathbb{Z}$. Écrivons :

$$[i]_{q^d-1} = s_0 + s_1 q + \cdots + s_{d-1} q^{d-1},$$

avec $0 \leq s_i \leq q-1$ pour $i = 0, \cdots, d-1$. On définit la somme de Gauss-Thakur associée à χ par :

$$\tau(\chi) = \prod_{i=0}^{d-1} \Big(- \sum_{\sigma \in G} \theta^{-q^i}(\sigma)\sigma(\lambda_P)\Big)^{s_i}.$$

Notons que si χ_0 est le caractère trivial alors $\tau(\chi_0) = 1$.

Lemme 2.1.
(i) $\forall \chi \in \widehat{G}$, $F(\tau(\chi)) = \tau(\chi^q)$.
(ii) $\forall \sigma \in G$, $\forall \chi \in \widehat{G}$, $\sigma(\tau(\chi)) = \chi(\sigma)\tau(\chi)$.

Preuve.
(i) Soit $i \in \mathbb{Z}$ tel que $\chi = \theta^i$, alors $\chi^q = \theta^{iq}$. Écrivons :

$$[i]_{q^d-1} = s_0 + \cdots + s_{d-1} q^{d-1},$$

alors :

$$[iq]_{q^d-1} = s_{d-1} + s_0 q + \cdots + s_{d-2} q^{d-2}.$$

Posons $s_{-1} = s_{d-1}$, alors :

$$\tau(\chi^q) = \prod_{i=0}^{d-1} \Big(- \sum_{\sigma \in G} \theta^{-q^i}(\sigma)\sigma(\lambda_P)\Big)^{s_{i-1}}.$$

D'où :

$$\tau(\chi^q) = \prod_{i=0}^{d-1} \Big(F\Big(- \sum_{\sigma \in G} \theta^{-q^{i-1}}(\sigma)\sigma(\lambda_P)\Big)\Big)^{s_{i-1}} = F(\tau(\chi)).$$

(ii) Soit $\delta \in G$. On a :

$$\delta(- \sum_{\sigma \in G} \theta^{-q^i}(\sigma)\sigma(\lambda_P)) = \theta^{q^i}(\delta)\Big(- \sum_{\sigma \in G} \theta^{-q^i}(\sigma)\sigma(\lambda_P)\Big).$$

Soient donc $\chi \in \widehat{G}$ et $i \in \mathbb{Z}$ tels que $\chi = \theta^i$. Écrivons $[i]_{q^d-1} = s_0 + \cdots + s_{d-1}q^{d-1}$. On a :

$$\delta(\tau(\chi)) = \tau(\chi) \prod_{i=0}^{d-1} \theta^{s_i q^i}(\delta) = \chi(\delta)\tau(\chi).$$

□

Soient $x \in K(d)$ et $\chi \in \widehat{G}$. On pose :

$$(x \mid \chi) = \sum_{\sigma \in G} \sigma(x)\chi^{-1}(\sigma).$$

Corollaire 2.2. *Soient* $\chi, \psi \in \widehat{G}$.
(i) *Si* $\chi \neq \psi$, *alors* $(\tau(\chi) \mid \psi) = 0$.
(ii) $(\tau(\chi) \mid \chi) = -\tau(\chi)$.

Preuve. Si on applique le Lemme 2.1, on a :

$$(\tau(\chi) \mid \psi) = \sum_{\sigma \in G} \chi(\sigma)\tau(\chi)\psi^{-1}(\sigma).$$

Or, si $\chi \neq \psi$:

$$\sum_{\sigma \in G} \chi(\sigma)\psi^{-1}(\sigma) = 0.$$

Et si $\chi = \psi$, on a :

$$\sum_{\sigma \in G} \chi(\sigma)\psi^{-1}(\sigma) = -1.$$

Le Corollaire suit. □

Proposition 2.3. *Soit* $\chi \in \widehat{G}$, χ *non trivial. Alors :*

$$\tau(\chi)\tau(\chi^{-1}) = (-1)^d P.$$

Preuve. Posons $\chi = \theta^i$. Alors $\chi^{-1} = \theta^{q^d-1-i}$. Écrivons :

$$[i]_{q^d-1} = s_0 + \cdots + s_{d-1}q^{d-1}.$$

Alors :

$$[q^d - 1 - i]_{q^d-1} = q^d - 1 - [i]_{q^d-1} = ((q-1) - s_0) + \cdots + ((q-1)s_{d-1})q^{d-1}.$$

Il suit :

$$\tau(\chi)\tau(\chi^{-1}) = \prod_{i=0}^{d-1}(-\sum_{\sigma\in G}\chi^{-q^i}(\sigma)\sigma(\lambda_P))^{q-1}.$$

Il reste à appliquer [13], Theorem II. □

Soit k une extension finie de Q, $k \subset K$. Notons $n = [k : Q]$. On pose :

$$\eta_k = \sum_{i=0}^{n-1}\tau(\theta^{i(q^d-1)/n}).$$

Lemme 2.4. $\eta_k \in O_k$.

Preuve. Si on applique le Lemme 2.1, on a :

$$F(\eta_k) = \eta_k.$$

Donc $\eta_k \in O_K$. De plus $\mathrm{Gal}(K/k) = G^n$. Ainsi, si on applique à nouveau le Lemme 2.1, on a $\eta_k \in O_k$. □

Théorème 2.5. *L'anneau O_k est un $Z[\mathrm{Gal}(k/Q)]$-module libre engendré par η_k.*

Preuve. Posons :

$$\eta_P = \eta_K = \sum_{i=0}^{q^d-2}\tau(\theta^i).$$

Soit R le $Z[G]$-module engendré par η_P. Il est clair que R est contenu dans O_K. Pour montrer la réciproque, il nous faut calculer le discriminant du Z-module R. Donc, nous devons calculer :

$$\mathrm{Det}((\sigma\delta(\eta_P))_{\sigma,\delta\in G})^2.$$

Or :

$$\mathrm{Det}(\sigma\delta(\eta_P))_{\sigma,\delta\in G}) = \prod_{\chi\in\widehat{G}}(\eta_P \mid \chi).$$

Par le Corollaire 2.2, on a :

$$(\eta_P \mid \chi) = -\tau(\chi).$$

D' où :

$$\mathrm{Det}((\sigma\delta(\eta_P))_{\sigma,\delta\in G})^2 = \prod_{\chi\in\widehat{G}}\tau(\chi)\tau(\chi^{-1}).$$

On applique alors la Proposition 2.3, on a :

$$\mathrm{Det}((\sigma\delta(\eta_P))_{\sigma,\delta\in G})^2 = (-1)^d P^{q^d-2}.$$

Ainsi les Z-modules R et O_K ont même discriminant. Donc $R = O_K$. Notons que :

$$\mathrm{Tr}_{K/k}(\eta_P) = \frac{-1}{n}\eta_k.$$

Le Théorème suit. $\square$

Notons que $\eta_P = \eta_K$ est essentiellement l'élément construit par Robin J. Chapman dans [4], Theorem 4.

Nous finissons ce paragraphe par la factorisation des sommes de Gauss-Thakur.

Théorème 2.6. *Soit $\mathcal{U}$ l'unique premier de $K(d)$ au dessus de $T-\omega$. Alors:*

$$\tau(\theta^i)O_{K(d)} = \mathcal{U}^{\sum_{j=1}^{d}[iq^{d-j}]_{q^d-1}F^j}.$$

Preuve. Par [1], preuve du Theorem 3.2, page 267 (voir aussi [13]), l'exposant de $\mathcal{U}$ dans la décomposition en facteurs premiers de $\tau(\theta^{q^t})$ est égal à $[q^t]_{q^d-1}$. Ainsi par le Lemme 2.1 et la Proposition 2.3, on a :

$$\tau(\theta^{q^t})O_{K(d)} = \mathcal{U}^{\sum_{j=1}^{d}[q^tq^{d-j}]_{q^d-1}F^j}.$$

Passons au cas général. Notons que le Théorème est trivialement vrai si $i \equiv 0 \pmod{q^d-1}$. On suppose donc que $i \not\equiv 0 \pmod{q^d-1}$. Écrivons :

$$[i]_{q^d-1} = s_0 + \cdots + s_{d-1}q^{d-1}.$$

Il suit :

$$\tau(\theta^i) = \prod_{i=0}^{d-1}\tau(\theta^{q^i})^{s_i}.$$

Ainsi :

$$\tau(\theta^i)O_{K(d)} = \mathcal{U}^{\sum_{j=1}^{d}(\sum_{i=0}^{d-1} s_i[q^iq^{d-j}]_{q^d-1})F^j}.$$

Or :

$$\sum_{i=0}^{d-1} s_i[q^iq^{d-j}]_{q^d-1} \equiv iq^{d-j} \pmod{q^d-1},$$

et :

$$0 \leq \sum_{i=0}^{d-1} s_i[q^iq^{d-j}]_{q^d-1} < q^d-1.$$

Donc :

$$\sum_{i=0}^{d-1} s_i[q^iq^{d-j}]_{q^d-1} = [iq^{d-j}]_{q^d-1}.$$

Le Théorème suit. $\square$

3. Bases normales entières relatives

On considère la tour de corps :

$$Q \subset k \subset N \subset K,$$

avec $n = [k : Q]$, $\ell = [N : k]$, $n \geq 2$. On pose $\Sigma = \mathrm{Gal}(k/Q)$ et $\Delta = \mathrm{Gal}(N/k)$. Nous allons examiner la question suivante : O_N est-il un $O_k[\Delta]$-module libre ? Notons f l'ordre de q dans $(\mathbb{Z}/\ell\mathbb{Z})^*$. Notons $\mathcal{Q}_k$ l'unique premier de k au dessus de P.

Lemme 3.1. *Si $(q^d - 1)/(q-1)$ divise n alors O_N est un $O_k[\Delta]$-module libre.*

Preuve. Posons $t = [K : k]$. Rappelons que le sous-corps de K de degré $(q^d-1)/(q-1)$ sur Q est :

$$Q(\lambda_P^{q-1}).$$

Comme K/Q est cyclique et que t divise $q-1$, on a:

$$k = Q(\lambda_P^t).$$

Notons $\mu_t \subset \mathbb{F}_q^*$ le groupe des racines t-ièmes de l'unité, alors :

$$\mathrm{Gal}(K/k) \simeq \mu_t.$$

Pour $\alpha \in \mu_t$, notons σ_α l'élément de $\mathrm{Gal}(K/k)$ tel que :

$$\sigma_\alpha(\lambda_P) = \alpha\lambda_P.$$

Posons :

$$x = 1 + \lambda_P + \cdots + \lambda_P^{t-1}.$$

Soit $0 \leq j \leq t-1$, on a :

$$\sum_{\alpha \in \mu_t} \alpha^{-j}\sigma_\alpha(x) = t\lambda_P^j.$$

Comme $O_K = O_k[\lambda_P]$, on en déduit que O_K est un $O_k[\mathrm{Gal}(K/k)]$-module libre engendré par x. Le Lemme suit. $\square$

Proposition 3.2. *Supposons que $f = 1$ et que ℓ et $h(k)$ sont premiers entre eux. Alors O_N est un $O_k[\Delta]$-module libre.*

Preuve. On a donc ℓ divise $q-1$. Donc il existe $x \in O_N$ et $a \in O_k$ avec $x^\ell = a$ et :

$$N = k(x).$$

Notons que $\mathcal{Q}_k$ est un idéal principal, en fait il est engendré par $N_{K/k}(\lambda_P)$. Comme N/k est totalement ramifiée en $\mathcal{Q}_k$ et non ramifiée ailleurs sauf peut-être en les places de S_k, on peut supposer que :

$$aO_k = \mathcal{Q}_k^u I^\ell,$$

où $1 \leq u < \ell$, u premier à ℓ et I est un idéal de O_k premier à $\mathcal{Q}_k$. Soit π un générateur de $\mathcal{Q}_k$, on peut donc supposer :

$$a = \pi^u \varepsilon,$$

où $\varepsilon \in E_k$. Soient alors $v, w \in \mathbb{N}$ tels que $uv - \ell w = 1$. Posons :

$$y = \frac{x^v}{\pi^w}.$$

Alors yO_N est l'unique premier de N au dessus de P et :

$$y^\ell = \pi\varepsilon.$$

Donc on peut supposer :

$$a = \pi,$$

où π est un générateur de $\mathcal{Q}_k$. Posons alors :

$$z = 1 + x + \cdots + x^{\ell-1}.$$

Notons que $O_N = O_k[x]$. On montre, comme pour le Lemme 3.1, que O_N est $O_k[\Delta]$-module libre engendré par z. $\square$

Nous aurons besoin des deux Lemmes qui suivent.

Lemme 3.3. *Soit n un entier, $n \geq 1$. Alors $E_{k(n)} = \mathbb{F}_{q^n}^* E_k$.*

Preuve. Il est clair que $E_k \mathbb{F}_{q^n}^* \subset E_{k(n)}$. Notons aussi que $E_{k(n)}$ et E_k ont le même rang sur $\mathbb{Z}$: $\#(S_k) - 1$. Soit $a \in E_{k(n)}$ et soit $m \geq 1$ minimal tel que :

$$a^m \in E_k.$$

Comme $k(a) \subset k(n)$ et que le corps des constantes de $k(n)$ est $\mathbb{F}_{q^n}$, m divise $q^n - 1$. Soit alors F le Frobenius de $k(n)/k$, i.e. $F \in \mathrm{Gal}(k(n)/k)$ est tel que:

$$\forall \zeta \in \mathbb{F}_{q^n},\ F(\zeta) = \zeta^q.$$

Ainsi, il existe $\zeta \in \mathbb{F}_{q^n}^*$ tel que:

$$F(a) = \zeta a.$$

Soit alors $\delta \in \mathbb{F}_{q^n}$ tel que :

$$\mathbb{F}_{q^n} = \bigoplus_{i=0}^{n-1} \mathbb{F}_q \delta^{q^i}.$$

Posons $\delta_i = \delta^{q^i} = F^i(\delta)$ pour $i = 0, \cdots, n-1$. Comme $O_{k(n)} = O_k[\mathbb{F}_{q^n}]$, on peut écrire :

$$a = \sum_{i=0}^{n-1} u_i \delta_i,$$

où $u_i \in O_k$ pour $i = 0, \cdots, n-1$. Mais alors :

$$F(a) = \sum_{i=0}^{n-1} \zeta u_i \delta_i = \sum_{i=0}^{n-1} u_i \delta_{i+1},$$

où on a posé $\delta_n = \delta$. On en déduit :

$$a = u_0 (\sum_{i=0}^{n-1} \zeta^{-i} \delta_i).$$

Ainsi $a \in \mathbb{F}_{q^n}^* E_k$. □

Lemme 3.4. *Notons $e_\infty(k)$ l'indice de ramification de $1/T$ dans k. Alors :*

$$N_{k/Q}(E_k) = (\mathbb{F}_q^*)^{e_\infty(k)}.$$

Preuve. On a la suite exacte de Σ-modules :

$$1 \to E_k \to k^* \to P_k \to 1\,.$$

D'où la suite exacte :

$$1 \to \mathbb{F}_q^* \to Q^* \to P_k^\Sigma \to H^1(\Sigma, E_k) \to 1\,.$$

Il suit :

$$H^1(\Sigma, E_k) \simeq \frac{P_k^\Sigma}{I_Q},$$

où I_Q est vu comme plongé dans P_k. Or P_k^Σ / I_Q est cyclique d'ordre n engendré par la classe de $\mathcal{Q}_k$. Ainsi :

$$\#(H^1(\Sigma, E_k)) = n.$$

Mais, par la preuve de [12], Theorem 8.3, page 179, on a :

$$\frac{\#(H^2(\Sigma, E_k))}{\#(H^1(\Sigma, E_k))} = \frac{e_\infty(k)}{n}.$$

Le Lemme suit. □

Théorème 3.5. *On suppose que $\ell = s^t$, où s est un nombre premier et $t \geq 1$. On suppose que s divise n et que $q^f \not\equiv 1 \pmod{s^{t+1}}$.*
(i) *Si s ne divise pas $q-1$ alors O_N n'est pas un $O_k[\Delta]$-module libre.*
(ii) *Si s divise $q-1$, posons $n = s^m n_1$, avec n_1 non divisible par s. Si la valuation s-adique de $(q-1)/e_\infty(k)$ est plus petite que $t-m$, alors O_N n'est pas un $O_k[\Delta]$-module libre.*

Preuve. Considérons l'injection $\Delta \to (O_k[\Delta])^*$. Alors, cette application induit un morphisme $H^2(\Sigma, \Delta) \to H^2(\Sigma, (O_k[\Delta])^*)$. Ici Σ agit trivialement sur Δ et Σ agit sur $O_k[\Delta]$ via son action galoisienne sur O_k. Notons E l'ensemble constitué des idempotents primitifs de $k[\Delta]$. Notons que comme le corps de constantes de k est $\mathbb{F}_q$, on a :

$$\forall e \in E,\ e \in Q[\Delta].$$

Ainsi, pour tout $e \in E$, Σ agit trivialement sur e. Pour $e \in E$, posons :

$$L_e = k[\Delta]e.$$

Notons O_e la fermeture intégrale de $O_k e$ dans L_e, alors :

$$(O_k[\Delta])^* = \prod_{e \in E} O_e^*.$$

Notons $\mu(e)$ le groupe des racines de l'unités de O_e^*, alors par le Lemme 3.3, on a :

$$\forall e \in E,\ O_e^* = \mu(e)(E_k e).$$

Or pour $e \in E$, on a :

$$\mu(e) \subset Q[\Delta]e.$$

Donc, pour tout e dans E, Σ agit trivialement sur $\mu(e)$. Si on applique le Lemme 3.4, nous obtenons :

$$H^2(\Sigma, (O_k[\Delta])^* = \prod_{e \in E} \frac{\mu(e)}{\mu(e)^n((\mathbb{F}_q^*)^{e_\infty(k)}e)}.$$

Notons aussi que :

$$H^2(\Sigma, \Delta) = \frac{\Delta}{\Delta^n}.$$

Il suit que le morphisme $H^2(\Sigma, \Delta) \to H^2(\Sigma, (O_k[\Delta])^*)$ est l'application qui à $\delta \in \Delta/\Delta^n$ associe la classe de $(\delta e)_{e \in E}$ dans $\prod_{e \in E} \frac{\mu(e)}{\mu(e)^n((\mathbb{F}_q^*)^{e_\infty(k)}e)}$. Or Δ est un groupe cyclique d'ordre une puissance d'un nombre premier, donc il existe $e' \in E$ tel que le morphisme $\Delta \to \mu(e')$, $\delta \mapsto \delta e'$, soit une injection. En particulier, on a :

$$\mu(e') \simeq \mathbb{F}_{q^f}^*.$$

Il suit que Δ est isomorphe au s-sous-groupe de Sylow de $\mu(e')$. Vu les hypothèses du Théorème, on en déduit que le morphisme :

$$\frac{\Delta}{\Delta^n} \to \frac{\mu(e')}{\mu(e')^n((\mathbb{F}_q^*)^{e_\infty(k)}e')}$$

est une injection. Donc le morphisme $H^2(\Sigma, \Delta) \to H^2(\Sigma, (O_k[\Delta])^*)$ est une injection. Il suffit alors d'appliquer [2], Corollary 9.6. $\square$

4. Le cas où ℓ et n sont premiers entre eux

On garde les notations du chapitre précédent. Dans ce paragraphe, nous supposerons que ℓ et n sont premiers entre eux.

Pour $j = 1, \ldots, f$, posons :

$$P_j(T) = \prod_{k=0}^{(d/f)-1} (T - \omega^{q^{j+kf}}).$$

Alors $P_1(T), \dots, P_f(T)$ sont des polynômes irréductibles de $\mathbb{F}_{q^f}[T]$, et :

$$P(T) = P_1(T) \cdots P_f(T).$$

Pour $j = 1, \dots, f$, on note $\mathcal{P}_j$ (respectivement $\mathcal{T}_j$) l'unique premier de $N(f)$ (respectivement de $k(f)$) au dessus de $P_j(T)$. Notons que :

$$\mathcal{Q}_k O_{k(f)} = \mathcal{T}_1 \cdots \mathcal{T}_f,$$

et, pour $j = 1, \dots, f$, on a :

$$\mathcal{T}_j^n = P_j(T) O_{k(f)}.$$

Pour $x \in N(f)$ et $\chi \in \widehat{\Delta}$, on pose :

$$(x \mid \chi) = \sum_{\delta \in \Delta} \delta(x) \chi^{-1}(\delta),$$

où on a identifié Δ à $\mathrm{Gal}(N(f)/k(f))$.

Lemme 4.1. *Pour $i = 0, \dots, \ell - 1$, on a :*

$$\tau(\theta^{((q^d-1)/\ell)i}) O_{N(f)} = \prod_{j=1}^{f} \mathcal{P}_j^{n[iq^{f-j}]_\ell}.$$

Preuve. Soit L le sous-corps de K de degré ℓ sur Q. Comme ℓ et n sont premiers entre eux, on a :

$$N = Lk.$$

Il suit :

$$\Delta \simeq \mathrm{Gal}(L/Q).$$

Ainsi $\theta^{(q^d-1)/\ell}$ induit un élément de $\widehat{\Delta}$ qui engendre $\widehat{\Delta}$. Par le Lemme 2.4 :

$$\eta_L = \sum_{i=0}^{\ell-1} \tau(\theta^{((q^d-1)/\ell)i}) \in O_L \subset O_N.$$

On a :

$$(\eta_L \mid \chi) = \ell \tau(\theta^{((q^d-1)/\ell)i}),$$

si $\chi \in \widehat{\Delta}$ est induit par $\theta^{((q^d-1)/\ell)i}$. Ainsi :

$$\tau(\theta^{((q^d-1)/\ell)i}) \in O_{N(f)},$$

pour $i = 0, \dots, \ell - 1$. Comme f est l'ordre de q dans $(\mathbb{Z}/\ell\mathbb{Z})^*$, le Lemme résulte alors du Théorème 2.6. $\square$

Pour $\chi \in \widehat{\Delta}$, on pose :

$$(O_{N(f)} \mid \chi) = \{(x \mid \chi),\, x \in O_{N(f)}\}.$$

Il est clair que $(O_{N(f)} \mid \chi)$ est un $O_{k(f)}$-sous-module de rang 1 de $O_{N(f)}$, et, si χ est trivial, $(O_{N(f)} \mid \chi) = O_{k(f)}$.

Proposition 4.2. *Soit* $\chi \in \widehat{\Delta}$, χ *non trivial et tel que* χ *soit induit par* $\theta^{((q^d-1)/\ell)i}$, $1 \leq i < \ell$, *alors :*

$$(O_{N(f)} \mid \chi)O_{N(f)} = \prod_{j=1}^{f} \mathcal{P}_j^{[niq^{f-j}]_\ell}.$$

Preuve. La preuve de cette Proposition est similaire à celle de [9], Proposition 2.1. En particulier, seuls les premiers de $N(f)$ au dessus de P interviennent dans la décomposition en idéaux premiers de $(O_{N(f)} \mid \chi)O_{N(f)}$.

Fixons donc $1 \leq j \leq f$. Alors $\mathcal{P}_j$ correspond à un plongement de $N(f)$ dans $\bar{Q}_P$, où Q_P est le complété P-adique de Q et $\bar{Q}_P$ une clôture algébrique fixée de Q_P.

Notons $\widehat{N}$ le complété $\mathcal{P}_j$-adique de $N(f)$ et $\widehat{k}$ le complété $\mathcal{T}_j$-adique de $k(f)$. Notons aussi $\widehat{K}$ le complété λ_P-adique de K. Il existe $\lambda \in \widehat{K}$ tel que (voir [1], paragraphe 1) :

$$\lambda^{q^d-1} = -P,$$
$$\lambda \equiv \lambda_P \pmod{\lambda_P^q}.$$

Posons :

$$\pi = \lambda^{(q^d-1)/(n\ell)}.$$

Notons que :

$$\widehat{N} = Q_P(\pi),$$

et :

$$\widehat{k} = Q_P(\pi^\ell).$$

Soit $\rho : G \to \mathbb{F}_{q^d}^* \subset Q_P$ l'application donnée par :

$$\forall A \in Z \setminus PZ,\ \rho(\sigma_A) \equiv A \pmod{P}.$$

On a donc :

$$\forall \sigma \in G,\ \sigma(\pi) = \rho(\sigma)^{(q^d-1)/(n\ell)}\pi.$$

Travaillons dans $K(d)$. On a :

$$\theta(\sigma_A) \equiv A \pmod{\mathcal{U}},$$

où $\mathcal{U}$ est l'unique premier de $K(d)$ au dessus de $T-\omega$. Notons F le Frobenius de $K(d)/K$, on a :

$$\theta(\sigma_A) \equiv A^{q^{d-j}} \pmod{F^j(\mathcal{U})}.$$

Il suit :

$$\theta^{((q^d-1)/\ell)i}(\sigma_A) \equiv A^{iq^{f-j}((q^d-1)/\ell)} \pmod{\mathcal{P}_j}.$$

Soit donc $0 \leq m < \ell$, on a dans $\widehat{K}$:

$$(\pi^m \mid \chi) = \sum_{\delta \in \Delta} \chi^{-1}(\delta)\delta(\pi^m).$$

Or G^n se surjecte dans Δ, il suit :

$$(\pi^m \mid \chi) = \frac{1}{n} \sum_{\sigma \in G} \rho(\sigma)^{(m - niq^{f-j})((q^d-1)/\ell)} \pi^m.$$

Il suit que si $m \not\equiv niq^{f-j} \pmod{\ell}$, on a :

$$(\pi^m \mid \chi) = 0.$$

Si $k \equiv niq^{f-j} \pmod{\ell}$, on a :

$$(\pi^m \mid \chi) = \frac{-1}{n} \pi^m.$$

Ainsi l'exposant de $\mathcal{P}_j$ dans la décomposition en facteurs premiers de $(O_{N(f)} \mid \chi) O_{N(f)}$ est $[niq^{f-j}]_\ell$. □

Théorème 4.3.
(i) *Si O_N est un $O_k[\Delta]$-module libre alors :*

$$\prod_{j=1}^{f} \mathcal{T}_j^{\frac{1}{\ell}([niq^{f-j}]_\ell - n[iq^{f-j}]_\ell)}$$

est un idéal principal de $k(f)$ pour $i = 1, \ldots, \ell - 1$.
(ii) *Si $f = 1$ alors O_N est un $O_k[\Delta]$-module libre.*

Preuve. Supposons que O_N est un $O_k[\Delta]$-module libre, alors $O_{N(f)}$ est un $O_{k(f)}[\Delta]$-module libre. Or $O_{N(f)}$ est un $O_{k(f)}[\Delta]$-module libre si et seulement si pour tout $\chi \in \widehat{\Delta}$, χ non trivial, $(O_{N(f)} \mid \chi)$ est un $O_{k(f)}$-module libre.

Soit donc $\chi \in \widehat{\Delta}$, χ non trivial. Alors χ est induit par $\theta^{i((q^d-1)/\ell)}$, $1 \leq i < \ell$. Or d'après le Lemme 4.1, on a :

$$\tau(\theta^{i(q^d-1)/\ell)}) \in (O_{N(f)} \mid \chi).$$

Ainsi $\frac{1}{\tau(\theta^{i(q^d-1)/\ell)})}(O_{N(f)} \mid \chi)$ est un idéal de $O_{k(f)}$. Si on combine le Lemme 4.1 et la Proposition 4.2, nous avons :

$$(O_{N(f)} \mid \chi) \tau(\theta^{i(q^d-1)/\ell)})^{-1} = \prod_{j=1}^{f} \mathcal{T}_j^{\frac{1}{\ell}([niq^{f-j}]_\ell - n[iq^{f-j}]_\ell)}.$$

Le Théorème suit. □

Pour $i = 1, \ldots, \ell - 1$, on pose :

$$\mathcal{A}_i = \prod_{j=1}^{f} \mathcal{T}_j^{\frac{1}{\ell}([niq^{f-j}]_\ell - n[iq^{f-j}]_\ell)}.$$

Nous identifions Σ à $\mathrm{Gal}(k(f)/Q(f))$. On considère $I_{Q(f)}$ et P_k comme des sous-groupes de $P_{k(f)}$.

Proposition 4.4. *Rappelons que $e_\infty(k)$ est l'indice de ramification de $1/T$ dans k. On a :*
$$\#(\frac{P_{k(f)}^{\Sigma}}{P_k^{\Sigma} I_{Q(f)}}) = \frac{(n,q^f-1)(\frac{q^f-1}{(n,q^f-1)},\frac{q-1}{e_\infty(k)})}{q-1}.$$

Preuve. Notons tout d'abord que $P_k^{\Sigma} I_{Q(f)}/I_{Q(f)}$ est un groupe cyclique d'ordre n engendré par $\mathcal{Q}_k O_{k(f)}$. Rappelons que, par le Lemme 3.3, on a :
$$E_{k(f)} = \mathbb{F}_{q^f}^* E_k.$$
De plus, on a la suit exacte :
$$1 \to E_{k(f)} \to k(f)^* \to P_{k(f)} \to 1.$$
On en déduit :
$$H^1(\Sigma, E_{k(f)}) \simeq \frac{P_{k(f)}^{\Sigma}}{I_{Q(f)}}.$$
Or :
$$\#(H^1(\Sigma, E_{k(f)})) = \#(H^2(\Sigma, E_{k(f)}))\frac{\#(H^1(\Sigma, E_{k(f)}))}{\#(H^2(\Sigma, E_{k(f)}))}.$$
Mais Σ est cyclique et E_k est d'indice fini dans $E_{k(f)}$, donc :
$$\frac{\#(H^1(\Sigma, E_{k(f)}))}{\#(H^2(\Sigma, E_{k(f)}))} = \frac{\#(H^1(\Sigma, E_k))}{\#(H^2(\Sigma, E_k))}.$$
Or on a vu dans la preuve du Lemme 3.4 que :
$$\#(H^1(\Sigma, E_k)) = n.$$
Il suit :
$$\#(\frac{P_{k(f)}^{\Sigma}}{P_k^{\Sigma} I_{Q(f)}}) = \frac{\#(H^2(\Sigma, E_{k(f)}))}{\#(H^2(\Sigma, E_k))}.$$
Or, toujours par le Lemme 3.4 :
$$H^2(\Sigma, E_k) = \frac{\mathbb{F}_q^*}{(\mathbb{F}_q^*)^{e_\infty(k)}}.$$
De plus :
$$H^2(\Sigma, E_{k(f)}) = \frac{\mathbb{F}_{q^f}^*}{(\mathbb{F}_{q^f}^*)^n (\mathbb{F}_q^*)^{e_\infty(k)}}.$$
On a :
$$(\mathbb{F}_{q^f}^* : (\mathbb{F}_{q^f}^*)^n) = (n, q^f-1).$$
De plus :
$$((\mathbb{F}_{q^f}^*)^n (\mathbb{F}_q^*)^{e_\infty(k)} : (\mathbb{F}_{q^f}^*)^n) = \frac{q-1}{e_\infty(k)}(\frac{q^f-1}{(n,q^f-1)}, \frac{q-1}{e_\infty(k)})^{-1}.$$
La Proposition suit. □

Notons r le plus grand commun diviseur des nombres n et $[iq^j]_\ell - i$, $i = 1, \ldots, \ell-1$, $j = 1, \ldots, f$.

Proposition 4.5. *Supposons que $\mathcal{A}_1, \ldots, \mathcal{A}_{\ell-1}$ sont des idéaux principaux. Notons alors m le plus petit commun multiple des ordres de $\mathcal{A}_1, \ldots, \mathcal{A}_{\ell-1}$ dans $\frac{P^\Sigma_{k(f)}}{P^\Sigma_k I_{Q(f)}}$. Alors n/r divise m.*

Preuve. Notons que $P^\Sigma_{k(f)}/I_{Q(f)}$ est le produit direct de f groupes cycliques d'ordres n engendrés par les images de $\mathcal{T}_1, \ldots, \mathcal{T}_f$. De plus, $P^\Sigma_k I_{Q(f)}/I_{Q(f)}$ est le groupe cyclique d'ordre n engendré par $\mathcal{Q}_k O_{k(f)} = \mathcal{T}_1 \cdots \mathcal{T}_f$. Ainsi, pour $i = 1, \ldots, \ell-1$, $j = 1, \ldots, f$, on a :

$$\frac{m}{\ell}([niq^{f-j}]_\ell - n[iq^{f-j}]_\ell) \equiv \frac{m}{\ell}([ni]_\ell - ni) \pmod{n}.$$

Il suit :

$$m([niq^{f-j}]_\ell - [ni]_\ell) \equiv 0 \pmod{n},$$

pour $i = 1, \ldots, \ell-1$ $j = 1, \ldots, f$. Comme n et ℓ sont premiers entre eux, ni parcoure les classes non nulles de $\mathbb{Z}/\ell\mathbb{Z}$. La Proposition suit. □

Théorème 4.6. *On suppose $f \geq 2$. Supposons que $e_\infty(k) \geq 2$ ou que $q^f \not\equiv 1 \pmod{n(q-1)}$, alors O_N n'est pas un $O_k[\Delta]$-module libre.*

Preuve. Posons :

$$h = \frac{n(q-1)}{(n, q^f-1)\left(\frac{q^f-1}{(n,q^f-1)}, \frac{q-1}{e_\infty(k)}\right)}.$$

Sous les hypothèses du Théorème on a :

$$h \geq 2.$$

Supposons que O_N est un $O_k[\Delta]$-module libre. Alors, par le Théorème 4.3, $\mathcal{A}_1, \ldots, \mathcal{A}_{\ell-1}$ sont dans $P^\Sigma_{k(f)}$. Si on applique les Propositions 4.4 et 4.5, h divise r. Ainsi, pour $i = 1, \ldots, \ell-1$, $j = 1, \ldots, f$, h divise $[iq^j]_\ell - i$. Soit alors i_0 le plus grand entier non nul tel que :

$$i_0[q]_\ell \leq \ell.$$

Comme $f \geq 2$, on a :

$$1 \leq i_0 \leq \ell - 2.$$

De plus :

$$[(i_0+1)[q]_\ell]_\ell = (i_0+1)[q]_\ell - \ell.$$

Or :

$$[(i_0+1)[q]_\ell]_\ell = [(i_0+1)q]_\ell.$$

Donc:

$$[(i_0+1)q]_\ell - (i_0+1) = (i_0+1)([q]_\ell - 1) - \ell.$$

Or h divise $[q]_\ell - 1$ et comme $i_0+1 \leq \ell-1$, h divise $[(i_0+1)q]_\ell - (i_0+1)$. Ceci entraîne que h divise ℓ, ce qui est contradictoire car h et ℓ sont premiers entre eux (h divise n). □

5. Le sous-corps quadratique de K

Nous supposons maintenant que q est impair. Soit alors k le sous-corps de K de degré deux sur Q. Par la théorie du corps de classes on a $k = Q(\sqrt{P})$ si $d = \mathrm{degP}$ est pair et $k = Q(\sqrt{-P})$ si d est impair.

Proposition 5.1. *Supposons que $d \leq 2$. Alors O_K est un $O_k[\Delta]$-module libre.*

Preuve. On vérifie facilement que k est de genre zéro. Ceci entraîne que pour tout entier $n \geq 1$, $O_{k(n)}$ est un anneau principal. Ainsi le groupe des classes de $O_k[\mathrm{Gal}(K/k)]$ est trivial. La Proposition suit. □

Théorème 5.2. *Supposons $d \geq 3$. Alors O_K n'est pas un $O_k[\mathrm{Gal}(K/k)]$-module libre.*

Preuve. Nous allons considérer deux cas.
• d n'est pas une puissance de deux . Écrivons $d = 2^m d'$ avec d' impair. Posons :

$$\ell = \frac{q^{d'} - 1}{q - 1}.$$

Notons que ℓ est un nombre impair. Soit alors L le sous-corps de K de degré ℓ sur Q et posons :

$$N = kL.$$

Alors :

$$[N : k] = \ell.$$

De plus, l'ordre de q dans $(\mathbb{Z}/\ell\mathbb{Z})^*$ est égal à $d' \geq 2$. Comme $q^{d'} \not\equiv 1 \pmod{2(q-1)}$, par le Théorème 4.6, O_N n'est pas un $O_k[\mathrm{Gal}(N/k)]$-module libre. Donc, a fortiori, O_K n'est pas un $O_k[\mathrm{Gal}(K/k)]$-module libre.
• d est une puissance de deux. Soit t la valuation 2-adique de $q^{d/2} - 1$. Posons $\ell = 2^t$. Notons que :

$$q^d \equiv 1 \pmod{2\ell}.$$

Soit N le sous-corps de K de degré 2ℓ sur Q. Alors $k \subset N$ et $[N : k] = \ell$. Notons que l'ordre de q dans $(\mathbb{Z}/\ell\mathbb{Z})^*$ est $d/2$. De plus :

$$q^{d/2} \not\equiv 1 \pmod{2^{t+1}}.$$

Notons que $e_\infty(k) = 1$. Comme $d/2 \geq 2$, la valuation 2-adique de $q - 1$ est inférieure à $t - 1$. Donc, si on applique le Théorème 3.5, O_N n'est pas un $O_k[\mathrm{Gal}(N/k)]$-module libre. Le Théorème suit. □

Bibliographie

[1] B. Anglès, *On the orthogonal of cyclotomic units in positive characteristic.* J. Number Theory **79** (1999), 258–283.

[2] J. Brinkhuis, *Galois modules and embedding problems.* J. Reine Ang. Math, **346** (1984), 141–164.

[3] J. Brinkhuis, *Normal integral bases and complex conjugation.* J. Reine Ang. Math **375/376** (1987), 157–166.

[4] R. J. Chapman, *Carlitz modules and normal integral bases.* J. London Math. Soc. **44** (1991), 250–260.

[5] J. Cougnard, *Bases normales relatives dans certaines extensions cyclotomiques.* J. Number Theory **23** (1986), 336–346.

[6] J. Cougnard, *Nouveaux exemples d'extensions relatives sans base normale.* preprint 2001.

[7] A. Fröhlich, *Galois module sructure of algebraic integers.* Springer-Verlag, 1983.

[8] D. Goss, *Basic structures of function field arithmetic.* Springer-Verlag, 1996.

[9] C. Greither, Relative integral normal bases in $\mathbb{Q}(\zeta_p)$, J. Number Theory **35** (1990), 180–193.

[10] C. Greither, D. R. Replogle, K. Rubin, A. Srivastav, *Swan modules and Hilbert-Speiser number fields.* J. Number Theory **79** (1999), 164–173.

[11] D. Hayes, *Explicit class field theory for rational function fields.* Trans. Amer. Math. soc. **189** (1974), 77–91.

[12] J. T. Tate, *Global class field theory.* In Algebraic Number Theory, edited by J. W. S. Cassels and A. Fröhlich, Academic Press, 162–203, 1967.

[13] D. Thakur, *Gauss sums for* $\mathbb{F}_q[T]$. Invent. Math. **94** (1988), 105–112.

Bruno Anglès
Université de Caen
Département de Mathématique et Mécanique
Campus II, Boulevard Maréchal Juin
BP 5186, 14032 Caen Cedex, France
E-mail : `angles@math.unicaen.fr`