p-extensions faiblement ramifies

Stéphane Vinatier*

Résumé : on fait le point des résultats connus sur la structure galoisienne de la racine carrée de la codifférente d'une p-extension faiblement ramifiée de $\mathbb{Q}$ et on esquisse une stratégie pour les améliorer.

1 La question

Etant donné un nombre premier p impair, on considère une p-extension finie galoisienne $N/\mathbb{Q}$, dont on note G le groupe de Galois et que l'on suppose *faiblement ramifiée*, ce qui revient à dire ici que le second groupe de ramification en p dans $N/\mathbb{Q}$ est trivial.

Comme G est d'ordre impair, on sait par la formule de Hilbert pour la valuation de la différente $\mathcal{D}$ de l'extension qu'il existe un idéal fractionnaire $\mathcal{A}$ de N qui vérifie l'égalité :

$$\mathcal{A}^2 = \mathcal{D}^{-1}$$

et que l'on appelle l'idéal *racine carrée de la codifférente*. De par sa définition, $\mathcal{A}$ est stable sous l'action de G et, comme pour l'anneau d'entiers $\mathcal{O}$ de N, se pose la question de sa structure en tant que $\mathbb{Z}[G]$-module.

Erez a montré [E] que notre hypothèse de ramification faible est nécessaire et suffisante pour que $\mathcal{A}$ soit un $\mathbb{Z}[G]$-module localement libre, c'est-à-dire pour qu'en tout premier l, $\mathcal{A}\otimes_{\mathbb{Z}}\mathbb{Z}_l$ soit un $\mathbb{Z}_l[G]$-module libre. On se penche dans cet article sur la question suivante : sous nos hypothèses, le $\mathbb{Z}[G]$-module $\mathcal{A}$ est-il libre, c'est-à-dire la racine carrée de la codifférente a-t-elle une base normale ? On dispose d'une réponse positive à cette question en supposant de plus :

- que $N/\mathbb{Q}$ est modérée ou abélienne [E],
- que le groupe de décomposition Γ en p est abélien [V1].

Nous reviendrons sur le deuxième point plus loin. Commençons par donner les grandes lignes de la stratégie élaborée par Fröhlich [F] et Taylor [Tay] pour étudier la structure galoisienne de l'anneau d'entiers, qu'Erez a appliquée à la racine carrée de la codifférente. Comme $\mathcal{A}$ est un $\mathbb{Z}[G]$-module localement libre, on peut considérer sa classe $(\mathcal{A})$ dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres $\mathrm{Cl}(\mathbb{Z}[G])$. L'ordre de G étant impair, on a l'équivalence :

$$\mathcal{A} \text{ est } \mathbb{Z}[G]\text{-libre } \Leftrightarrow \ (\mathcal{A}) = 1 \ ,$$

si bien que notre problème se ramène à l'étude de la classe $(\mathcal{A})$.

*Laboratoire A2X - Université Bordeaux 1

Pour mener celle-ci à bien, on utilise la Hom-description de Fröhlich, que l'on résume succintement par l'isomorphisme :

$$\mathrm{Cl}(\mathbb{Z}[G]) \simeq \frac{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^*)\mathrm{Det}(\mathbb{Z}[G]^*)} \ .$$

On note f l'élément de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$ qui représente $(\mathcal{A})$ à droite ; il s'agit donc d'une fonction définie sur le groupe des caractères virtuels R_G de G, à valeurs dans le groupe d'idèles d'un corps de nombres E "suffisamment gros", et qui commute à l'action du groupe de Galois absolu $\Omega_\mathbb{Q}$ de $\mathbb{Q}$.

Cette fonction a une composante en chaque place de E. Les résultats de Taylor et d'Erez permettent de traiter les composantes de f aux places modérées. Le problème est donc d'étudier la p-composante f_p de f (à valeurs dans $J_p(E) \simeq \prod_{\mathfrak{p}|p} E_\mathfrak{p}^*$), et plus précisément son facteur "sauvage", que l'on va décrire plus bas. Notons pour l'instant qu'on peut voir f_p comme une fonction sur les caractères de Γ, le groupe de décomposition en p, et à valeurs dans E_p^*, le groupe multiplicatif de l'une (fixée à l'avance) des extensions complétées de E au-dessus de $\mathbb{Q}_p$. Dans ces nouveaux termes, notre question devient :

$$\text{a-t-on } f_p \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma, E^*)\mathrm{Det}(\mathbb{Z}_p[\Gamma]^*) \, ?$$

En effet, la classe $(\mathcal{A})$ est triviale si et seulement si chaque composante de f se trouve dans la composante correspondante du dénominateur du quotient de la Hom-description. Le résultat suivant d'Erez [E, théorème 2.7] est un premier pas vers la réponse et nous donne l'occasion de décrire succintement le groupe Det. Il stipule que, si $\mathcal{M}$ désigne un ordre maximal de $\mathbb{Q}_p[\Gamma]$ contenant $\mathbb{Z}_p[\Gamma]$, alors :

$$f_p \in \mathrm{Det}(\mathcal{M}^*) \ ,$$

c'est-à-dire qu'il existe un élément $x \in \mathcal{M}^*$ (donc x peut s'écrire $x = \sum_\Gamma x_\gamma \gamma$, avec les $x_\gamma \in \mathbb{Q}_p$) tel que, si χ est le caractère d'une représentation matricielle T de Γ, alors $f_p(\chi) = \mathrm{Det}_\chi(x)$ où, par définition :

$$\mathrm{Det}_\chi(x) = \det\Big(\sum_\Gamma x_\gamma T(\gamma)\Big) \ .$$

Donnons-nous un tel $x \in \mathcal{M}^*$; la question est maintenant de savoir si $x \in \mathbb{Z}_p[\Gamma]^*$.

2 Investigations locales

L'isomorphisme de la Hom-description a l'avantage d'être explicite, c'est-à-dire qu'il donne un moyen de construire la fonction f qui représente la classe $(\mathcal{A})$. Dans cette partie, on décrit le facteur sauvage de la p-composante f_p de f, puis on montre comment l'estimer dans deux situations différentes, ce qui amène deux réponses (dont l'une est partielle) à la question posée.

2.1 Le représentant de la classe $(\mathcal{A})$

On commence par fixer quelques notations. Soit N_p l'extension complétée de N en une place divisant p ; le groupe de décomposition Γ en p dans $N/\mathbb{Q}$ s'identifie alors à $\mathrm{Gal}(N_p/\mathbb{Q}_p)$. Le fait que $\mathcal{A}$ soit localement libre entraîne que la

racine carrée de la codifférente de l'extension locale $\mathcal{A}_{N_p/\mathbb{Q}_p}$ est un $\mathbb{Z}_p[\Gamma]$-module libre [E] ; on désigne par α_p une base normale de $\mathcal{A}_{N_p/\mathbb{Q}_p}$. On peut maintenant décrire le premier ingrédient rentrant dans la composition de f_p, la résolvante associée à α_p. Si χ est le caractère d'une représentation matricielle T de Γ, elle est donnée par :

$$(\alpha_p \,|\, \chi) = \det\Big(\sum_{\Gamma} \gamma(\alpha_p) T(\gamma^{-1})\Big) \ .$$

Le second ingrédient qui intervient est la somme de Gauss locale τ_p [Tat, p.94], tordue par la seconde opération d'Adams ψ. Celle-ci agit sur le groupe des caractères virtuels R_Γ de Γ par $\psi(\chi)(\gamma) = \chi(\gamma^2)$, pour $\chi \in R_\Gamma$ et $\gamma \in \Gamma$. Le facteur sauvage de la p-composante de f, que l'on note encore f_p par abus de notation, est alors la fonction définie pour $\chi \in R_\Gamma$ par :

$$f_p(\chi) = (\alpha_p \,|\, \chi)\tau_p(\chi - \psi(\chi)) \ .$$

2.2 Cas Γ abélien

Lorsque le groupe de décomposition en la seule place sauvage p est abélien, on dispose d'une réponse complète à la question posée [V1, théorème 1.2].

Théorème 1 *Si Γ est abélien, alors $(\mathcal{A}) = 1$.*

Donnons quelques éléments de la preuve de ce résultat. Nos hypothèses entraînent que $N_p/\mathbb{Q}_p$ est abélienne faiblement ramifiée. Or, on peut décrire toutes les extensions abéliennes faiblement ramifiées de $\mathbb{Q}_p$ [V1, théorème 1.1], à l'aide de la théorie de Kronecker-Weber, ce qui permet de ramener le calcul de f_p au cas particulier où N_p est l'unique sous-extension L de $\mathbb{Q}_p(\zeta_{p^2})$ de degré p, ζ_{p^2} étant une racine primitive p^2-ième de l'unité. On note f_L la fonction sur les caractères de $C_p = \mathrm{Gal}(L/\mathbb{Q}_p)$ correspondante. On connaît explicitement une base normale α_L de $\mathcal{A}_{L/\mathbb{Q}_p}$:

$$\alpha_L = \frac{1}{p}\big(1 + \mathrm{tr}_{\mathbb{Q}_p(\zeta_{p^2})/L}(\zeta_{p^2})\big) \ . \tag{1}$$

On en déduit l'expression suivante de f_L, pour χ caractère de C_p :

$$f_L(\chi) = (\alpha_L \,|\, \chi)\tau_p(\chi - \psi(\chi)) = \chi\Big(\frac{p^2}{4u}\Big){\zeta_{p^2}}^{pv} \ , \tag{2}$$

où u et v sont des entiers. Il reste à prouver que cette fonction est dans la p-composante du dénominateur de la Hom-description de $\mathrm{Cl}(\mathbb{Z}[C_p])$. Soient $\mathcal{M}$ l'ordre maximal de $\mathbb{Q}_p[C_p]$ et $x \in \mathcal{M}^*$ tel que $f_L(\chi) = \mathrm{Det}_\chi(x)$. Soit ζ_p une racine primitive p-ième de l'unité, on a la décomposition :

$$\mathbb{Z}_p[C_p] \hookrightarrow \mathbb{Z}_p \oplus \mathbb{Z}_p[\zeta_p] \simeq \mathcal{M} \ni x \ .$$

De plus, si θ est un générateur du groupe des caractères irréductibles de C_p :

$$x \in \mathbb{Z}_p[C_p] \Leftrightarrow \mathrm{Det}_1(x) \equiv \mathrm{Det}_\theta(x) \bmod (1-\zeta_p) \ . \tag{3}$$

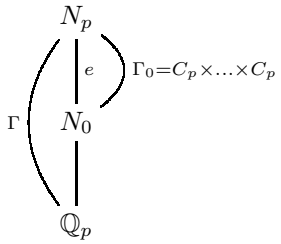
Or $\mathrm{Det}_1(x) = f_L(1) = 1$ et $\mathrm{Det}_\theta(x) = f_L(\theta)$ est une racine p-ième de l'unité d'après (2), donc $x \in \mathcal{M}^* \cap \mathbb{Z}_p[C_p] = \mathbb{Z}_p[C_p]^*$ et $f_L \in \mathrm{Det}(\mathbb{Z}_p[C_p]^*)$. Le théorème s'en déduit à l'aide des propriétés fonctorielles de la Hom-description (pour revenir à la fonction f_p) et de résultats similaires pour les composantes de f aux places modérées.

2.3 Cas Γ non abélien

Le résultat dont on dispose dans ce cas est moins fort, c'est une majoration de l'ordre de $(\mathcal{A})$ dans $\mathrm{Cl}(\mathbb{Z}[G])$ [V2, théorème 1].

Théorème 2 *Soit e l'indice de ramification en p dans $N/\mathbb{Q}$, on a $(\mathcal{A})^e = 1$.*

Le diagramme suivant donne une idée de la situation. Γ n'est plus abélien mais comme $N_p/\mathbb{Q}_p$ est une p-extension faiblement ramifiée, il est facile de voir que son groupe d'inertie Γ_0 est abélien p-élémentaire. On fait donc en sorte de se ramener à des fonctions définies sur les caractères de Γ_0 :



où N_0 est la sous-extension de $N_p/\mathbb{Q}_p$ fixée par Γ_0. La difficulté par rapport à la situation précédente est que l'extension faiblement ramifiée abélienne N_p/N_0 n'est plus absolue et qu'on ne peut donc pas utiliser Kronecker-Weber pour en obtenir une description.

On commence par esquisser le traitement de la somme de Gauss. On peut montrer que les caractères irréductibles de Γ sont tous de la forme :

$$\chi = \mathrm{Ind}_{\Sigma}^{\Gamma}\varphi$$

où φ est un caractère irréductible de Γ_0 étendu en un caractère abélien de son stabilisateur Σ (pour l'action de Γ sur les caractères de Γ_0). Par inductivité en degré 0 de la somme de Gauss, on en déduit :

$$\tau_p(\chi - \psi(\chi)) = \tau_p(\varphi - \psi(\varphi)) = \frac{\tau_p(\varphi)}{\tau_p(\varphi^2)} = \frac{W(\overline{\varphi})}{W(\overline{\varphi}^2)} \ ,$$

vue la relation entre le "local root number" W et la somme de Gauss [Tat, p.94]. Le quotient obtenu est une racine de l'unité par [Tat, p.96]. En conjugant ce résultat et la formule d'action galoisienne sur la somme de Gauss [F, théorème 20B], on obtient [V2, proposition 2.5] :

Proposition 2.1 $\chi \mapsto \tau_p(\chi - \psi(\chi))^p \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{\Gamma}, \mathcal{O}_E^*)$.

Ce résultat suffit à régler le sort de la somme de Gauss (sa puissance p-ième se trouve dans le premier facteur du dénominateur de la Hom-description).

Venons en à la résolvante. Soit β_p une base de $\mathcal{A}_{N_p/\mathbb{Q}_p}$ comme $\mathcal{O}_{N_0}[\Gamma_0]$-module, on sait par [E, (6.3)] qu'il existe $\lambda \in \mathcal{O}_{N_0}[\Gamma]^*$ tel que, pour tout caractère χ de Γ :

$$(\alpha_p \,|\, \chi) = (\beta_p \,|\, \mathrm{Res}_{\Gamma_0}^{\Gamma}(\chi))\mathrm{Det}_{\chi}(\lambda)$$

La formule d'action galoisienne sur la résolvante [F, théorème 20A] et l'étude de sa valuation permettent de prouver [V2, lemme 2.9] :

Proposition 2.2 $\theta \mapsto (\beta_p \,|\, \theta)^p \in \mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0}, \mathcal{O}_{E_p}^*)$.

Or, si $\mathcal{M}_0$ est l'ordre maximal de $N_0[\Gamma_0]$, on sait que $\mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0}, \mathcal{O}_{E_p}^*) = \mathrm{Det}({\mathcal{M}_0}^*)$, donc il existe $x \in {\mathcal{M}_0}^*$ tel que $(\beta_p \,|\, \theta)^p = \mathrm{Det}_\theta(x)$ pour tout caractère θ de Γ_0. Notons $e = p^m$ et $r = 1 + p + \cdots + p^{m-1}$, on a la décomposition :

$$\mathcal{M}_0 \simeq \mathcal{O}_{N_0} \oplus \left({\mathcal{O}_{N_0(\zeta_p)}}^{\oplus r}\right) \ . \tag{4}$$

Le théorème de Jacobinski [CR, 27.8] décrit le conducteur de $\mathcal{M}_0$ dans $\mathcal{O}_{N_0}[\Gamma_0]$:

$$\mathcal{F} = \{a \in \mathcal{O}_{N_0}[\Gamma_0],\ a\mathcal{M}_0 \subset \mathcal{O}_{N_0}[\Gamma_0]\} = p^m \mathcal{O}_{N_0} \oplus \left(p^m \pi^{1-p} {\mathcal{O}_{N_0(\zeta_p)}}^{\oplus r}\right) \ ,$$

où π est une uniformisante de $N_0(\zeta_p)$. On note q le cardinal du corps résiduel de N_0. En considérant chaque composante de x dans (4), on en déduit $x^{(q-1)p^{m-1}} \in \mathcal{F}\mathcal{M}_0 = \mathcal{O}_{N_0}[\Gamma_0]$. Il ne reste qu'à noter que $\mathcal{O}_{N_0}[\Gamma_0]^* = \mathcal{O}_{N_0}[\Gamma_0] \cap {\mathcal{M}_0}^*$ pour obtenir :

$$\theta \mapsto (\beta_p \,|\, \theta)^{(q-1)e} \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma_0]^*) \ .$$

Les techniques usuelles, plus le fait que le groupe noyau $\mathcal{D}(\mathbb{Z}[G])$ est un p-groupe lorsque G en est un [CR, 50.18], permettent alors de terminer la preuve du théorème 2.

3 Comment aller plus loin ?

Si l'on se satisfait du résultat concernant la somme de Gauss (proposition 2.1), pour laquelle on peut par ailleurs obtenir une expression explicite en utilisant [Tat, p.94, proposition 1], on a besoin de préciser celui concernant la résolvante. Le problème est de montrer que $(\beta_p \,|\, \theta) \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma_0]^*)$. Dans le cas où Γ est abélien (partie 2.2), la théorie de Kronecker-Weber permet de décrire l'extension $N_p/\mathbb{Q}_p$, si bien que l'on dispose d'une formule explicite pour la base normale, ce qui rend possible le calcul de la résolvante associée.

Si $N/\mathbb{Q}$ n'est pas totalement ramifiée en p, la théorie de Kronecker-Weber ne permet pas de décrire l'extension N_p/N_0, ni bien sûr de trouver une base normale pour $\mathcal{A}_{N_p/N_0}$. Un résultat de Byott [B] montre que la théorie de Lubin-Tate est bien adaptée pour prendre la relève. Expliquons brièvement comment (on peut se reporter à [S1] pour des détails sur cette théorie). Soit k une extension finie de $\mathbb{Q}_p$, q le cardinal de son corps résiduel, π une uniformisante de k et f_π le polynôme :

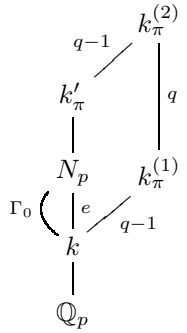
$$f_\pi(X) = \pi X + X^q \ .$$

Soit $\mathfrak{p}$ l'idéal maximal de l'anneau d'entiers d'une clôture algébrique de k. Pour tout entier $n \geq 1$, on note $f_\pi^{(n)} = f_\pi \circ \cdots \circ f_\pi$ l'itérée n-ième de f_π et on pose :

$$G_\pi^{(n)} = \{\omega \in \mathfrak{p},\ f_\pi^{(n)}(\omega) = 0\} \ .$$

Alors $k_\pi^{(n)} = k(G_\pi^{(n)})$ est le n-ième corps de division associé à la série de Lubin-Tate f_π. En particulier, $k_\pi^{(2)}$ est une extension abélienne totalement ramifiée de k de degré $q(q-1)$; notons k'_π l'unique sous-extension de $k_\pi^{(2)}$ de degré q sur k. On déduit de [B, lemme 4.2] que pour toute extension abélienne totalement et faiblement ramifiée F de k, on peut choisir l'uniformisante π de sorte que

$F \subset k'_\pi$. Ceci est vrai en particulier pour l'extension N_p/N_0 (avec $k = N_0$), on a alors le diagramme :



On peut donc appliquer le théorème 2 de [B], qui assure que toute uniformisante de N_p engendre l'anneau d'entiers $\mathcal{O}_{N_p}$ comme module sur son ordre associé. On note $\mathcal{P}$ (resp. $\wp$) l'idéal premier de $\mathcal{O}_{N_p}$ (resp. $\mathcal{O}_{N_0}$) et on en déduit :

Proposition 3.1 *Toute uniformisante β de N_p est une base normale pour $\mathcal{P}$ sur $\mathcal{O}_{N_0}$, c'est-à-dire $\mathcal{P} = \mathcal{O}_{N_0}[\Gamma_0]\beta$.*

On sait par [U, théorème 2] que, comme N_p/N_0 est totalement et faiblement ramifiée, $\mathcal{P}$ est un $\mathcal{O}_{N_0}[\Gamma_0]$-module libre ; cette proposition fournit des générateurs.

Preuve. L'ordre associé à l'anneau d'entiers est [B, lemme 3.1] :

$$\mathcal{U}_{N_p/N_0} = \{x \in N_0[\Gamma_0],\ x\mathcal{O}_{N_p} \subset \mathcal{O}_{N_p}\} = \mathcal{O}_{N_0}[\Gamma_0] + \mathcal{O}_{N_0}(\pi^{-1}T_{\Gamma_0}) \ ,$$

où π est une uniformisante de N_0 et $T_{\Gamma_0} = \sum_{\gamma\in\Gamma_0}\gamma$. Donc, si β est une uniformisante de N_p, tout $x \in \mathcal{P} \subset \mathcal{O}_{N_p}$ s'écrit :

$$x = \sum_{\gamma\in\Gamma_0} n_\gamma\gamma(\beta) + y\,\pi^{-1}T_{\Gamma_0}(\beta) \ ,$$

avec $n_\gamma \in \mathcal{O}_{N_0}$ pour tout $\gamma \in \Gamma_0$ et $y \in \mathcal{O}_{N_0}$. On note que $\sum_{\Gamma_0} n_\gamma\gamma(\beta) \in \mathcal{P}$, donc $y\,\pi^{-1}T_{\Gamma_0}(\beta) \in \mathcal{P} \cap \mathcal{O}_{N_0} = \wp$. Montrons que $\pi^{-1}T_{\Gamma_0}(\beta) \in \mathcal{O}_{N_0}^*$: en tenant compte du fait que N_p/N_0 est faiblement ramifiée, on tire aisément de [S2, III, proposition 7] que $\mathrm{tr}_{N_p/N_0}(\mathcal{P}) = \wp$ et $\mathrm{tr}_{N_p/N_0}(\mathcal{P}^2) = \wp^2$. En passant au quotient, on obtient donc une surjection :

$$\mathrm{tr}_{N_p/N_0} \ : \ \frac{\mathcal{P}}{\mathcal{P}^2} \longrightarrow\!\!\!\!\!\rightarrow \frac{\wp}{\wp^2} \ ,$$

dans laquelle les ensembles de départ et d'arrivée sont tous deux isomorphes au corps résiduel de N_0, donc cette application est une bijection. On en tire que $T_{\Gamma_0}(\beta) = \mathrm{tr}_{N_p/N_0}(\beta) \in \wp \setminus \wp^2$ comme annoncé, d'où il s'ensuit que $y \in \wp$. On l'écrit $y = \pi z$ avec $z \in \mathcal{O}_{N_0}$ et on obtient $x = \sum_{\Gamma_0}(n_\gamma + z)\gamma(\beta)$. On a ainsi montré que $\mathcal{P} \subset \mathcal{O}_{N_0}[\Gamma_0]\,\beta$, ce qui entraîne la proposition. ∎

Comme $\mathcal{A}_{N_p/N_0} = \mathcal{P}^{1-e} = p^{-1}\mathcal{P}$, on obtient immédiatement :

Corollaire 3.2 *Soit β une uniformisante de N_p, alors $\alpha = \dfrac{\beta}{p}$ est une base normale de $\mathcal{A}_{N_p/N_0}$, c'est-à-dire $\mathcal{A}_{N_p/N_0} = \mathcal{O}_{N_0}[\Gamma_0]\,\alpha$.*

En particulier, on sait que tout $\omega \in G^{(2)} \setminus G^{(1)}$ est une uniformisante de $k_\pi^{(2)}$. On en déduit que

$$\omega' = \mathrm{N}_{k_\pi^{(2)}/k'_\pi}(\omega) = \omega^{q-1} \tag{5}$$

est une uniformisante de k'_π, et donc $\alpha = \dfrac{\omega'}{p}$ est une base normale de $\mathcal{A}_{k'/k}$.

Il reste à calculer la résolvante $(\alpha \,|\, \chi)$ associée à α, pour χ caractère de $\mathrm{Gal}(k'/k)$. Les éléments de ce groupe de Galois et leur action sur α peuvent être décrits à l'aide de la loi de groupe formel pour laquelle f_π est un endomorphisme (voir [S1]). Malheureusement, les calculs s'avèrent nettement plus difficiles que dans le cas cyclotomique (partie 2.2). D'une part parce que la loi de groupe formel associée à notre choix de f_π est une série formelle avec une infinité de termes, si bien qu'on peut seulement espérer estimer la résolvante modulo une puissance de l'uniformisante de $k'_\pi(\zeta_p)$; d'autre part parce que la base normale est exprimée ici comme norme d'un élément sur lequel on connaît l'action du groupe de Galois (5), alors que c'était une trace dans le cas cyclotomique (1). Des résultats partiels ont cependant été obtenus par l'auteur, qui espère parvenir à les compléter.

Références

[B] Byott N.P., Integral Galois module structure of some Lubin-Tate extensions, *J. Number Theory*, **77** (1999), *no. 2*, 252–273.

[CR] Curtis C. W., Reiner I., *Methods of representation theory, Vol. I & II*, Wiley, New York (1990).

[E] Erez B., A survey of recent work on the square root of the inverse different, Journées arithmétiques, Exp. Congr. Luminy (1989), *Astérisque*, **198-200**, 133–152.

[F] Fröhlich A., *Galois module structure of algebraic integers*, Ergebnisse der Mathematik, 3. Folge, Bd. 1, Springer, Berlin (1983).

[S1] Serre J.P., Local class field theory, in *Algebraic number theory*, eds. Cassels J.W.S. and Fröhlich A., Acad. Press, London (1967), 128–161.

[S2] Serre J.P., *Corps locaux*, 3e édition, Hermann, Paris (1968).

[Tat] Tate J.T., Local constants, in *Algebraic number fields (L-functions and Galois properties)*, ed. Fröhlich A., Acad. Press, London (1977), 89–131.

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

[U] Ullom S., Integral normal bases in Galois extensions of local fields, *Nagoya Math. J.* **39** (1970), 141–148.

[V1] Vinatier S., Structure galoisienne dans les extensions faiblement ramifiées de $\mathbb{Q}$, *J. Number Theory*, **91** (2001), *no. 1*, 126–152.

[V2] Vinatier S., Sur la racine carrée de la codifférente, Actes des J.A. Lille 2001, *à paraître au J. Théor. Nombres Bordeaux*.