THÉORIE DES NOMBRES
BESANÇON

Années 1996/97-1997/98

Extensions cycliques T-totalement ramifiées

G. GRAS
A. MUNNIER

Extensions cycliques T-totalement ramifiées

par

Georges GRAS et Adeline MUNNIER

1 Introduction

Soient k un corps de nombres, p un nombre premier, e un entier ≥ 1, et T un ensemble fini non vide d'idéaux premiers de k vérifiant $Nl \equiv 1 \bmod p^e$ pour tout $l \in T$ [1].

Nous nous proposons de donner, en termes de corps gouvernants (au sens de [4]), une condition nécessaire et suffisante à l'existence d'une extension k_e de k, cyclique de degré p^e, T-totalement ramifiée (i.e non ramifiée en dehors de T, non complexifiée (si $p = 2$), et telle que tout $l \in T$ soit totalement ramifié dans k_e/k).

La construction de ce type d'extension est liée au problème de principalisation étudié dans [2] : Dans cet article, étant donnés une extension abélienne finie F de k, de degré étranger à p, et un idéal $\mathfrak{a}$ de F, d'ordre p^e, $e \geq 1$, dans le groupe des classes de F, le premier auteur montre que l'on peut principaliser $\mathfrak{a}$ dans une extension de F, abélienne sur k, à partir d'extensions cycliques de degré p^e de k, T-totalement ramifiées. Pour ce faire, il utilise un ensemble fini T de places finies modérées de k, pour lequel, pour tout $l \in T$, il existe une extension cyclique $k_e(l)$ de k, de degré p^e, et $\{l\}$-totalement ramifiée ; ainsi, dans le composé direct des $k_e(l)$, $l \in T$, on peut trouver k_e, cyclique de degré p^e sur k, T-totalement ramifiée. Sous des conditions supplémentaires d'engendrement par les Frobenius des éléments de T, dans un corps gouvernant convenable, l'extension $K = k_e F$ principalise $\mathfrak{a}$.

La construction de k_e, via celle des $k_e(l)$, demande que les éléments de T vérifient des conditions simples à réaliser mais inutilement fortes [2] ; il est donc légitime de chercher à caractériser les parties T qui conduisent à l'existence d'au moins une extension cyclique de degré p^e, T-totalement ramifiée.

C'est le but de cet article qui s'appuie essentiellement sur une étude menée par le second auteur ; il généralise également un ancien problème posé dans [1], et résolu dans [1] et [4,th.6.1] pour le cas $|T| = 1$.

[1] Cette condition sur les normes absolues étant trivialement nécessaire pour le problème de ramification modérée étudié, il est plus simple de la supposer dès le départ.

[2] Ces conditions suffisantes sont rappelées dans la remarque (5.1).

Le résultat principal est constitué par l'énoncé suivant :

Théorème 1.1 *Soient k un corps de nombres, $A = \{\alpha \in k^\times, (\alpha)$ puissance p-ième d'idéal $\}$ et $E \subset A$ le groupe des unités de k.*

Soit $T = \{l_1, \ldots, l_n\}$ un ensemble de $n \geq 1$ idéaux premiers de k, tel que $Nl_i \equiv 1 \bmod p^e$, pour tout $i \in [1,n]$, soit $\{\mathfrak{L}_{1,e}, \ldots, \mathfrak{L}_{n,e}\}$ un ensemble de n idéaux premiers de $k(\mu_{p^e})$ tels que $\mathfrak{L}_{i,e} | l_i$ pour tout $i \in [1,n]$.

Alors il existe une extension cyclique de degré p^e de k, T-totalement ramifiée, si et seulement si il existe $(a_i)_{i\in[1,n]} \in (\mathbb{Z}/p^e\mathbb{Z})^n$, $a_i \not\equiv 0$ mod p, pour tout i, conduisant à la relation suivante, en termes de Frobenius :

$$\prod_{i=1}^{n} \left(\frac{k(\mu_{p^e}, (EA^{p^{e-1}})^{\frac{1}{p^e}})/k(\mu_{p^e})}{\mathfrak{L}_{i,e}} \right)^{a_i} = 1.$$

1.1 Notations et rappels

(i) Pour un corps de nombres k, nous notons :

E le groupe des unités de k,

$A = \{\alpha \in k^\times, (\alpha)$ puissance p-ième d'idéal $\}$,

k^{nr} le corps de classes absolu de Hilbert de k (pour lequel $\mathrm{Gal}(k^{\mathrm{nr}}/k)$ est isomorphe au groupe des classes de k).

(ii) Soit $T = \{l_1, \ldots, l_n\}$ un ensemble de $n \geq 1$ idéaux premiers de k tels que $Nl_i \equiv 1 \bmod p^e$, pour tout $i \in [1,n]$; on lui associe le module :

$$m = \prod_{i=1}^{n} l_i,$$

et on désigne par :

J_T le groupe des idéaux fractionnaires de k étrangers à T,

$k_T^\times = \{x \in k^\times, (x,T) = 1\}$,

$P_T = \{(x), x \in k_T^\times\}$,

$k_m^\times = \{x \in k_T^\times, x \equiv 1 \bmod m\}$,

$E_m = E \cap k_m^\times$,

$R_m = \{(x), x \in k_m^\times\}$,

$Cl_m = J_T/R_m$,

$A_T = A \cap k_T^\times$ (on a $A = A_T k^{\times p}$).

(iii) Par la théorie du corps de classes, il existe une extension abélienne de k, notée $k^{(m)}$, appelée le corps de classes de rayon m de k, telle que $\mathrm{Gal}(k^{(m)}/k) \simeq Cl_m$, l'isomorphisme étant réalisé via l'application d'Artin ; $k^{(m)}$ est aussi l'extension abélienne T-modérément ramifiée maximale de k (cf. [3, §1.1.2]).

(iv) Pour chaque $i \in [1,n]$, on note $\overline{k}_{l_i}$ le corps résiduel de k en l_i et I_{l_i} le groupe d'inertie de l_i dans $k^{(m)}/k$.

(v) Si Γ est un groupe abélien fini, on note Γ^* le groupe dual $\mathrm{Hom}(\Gamma, \mathbb{C}^\times)$, et pour tout homomorphisme de groupes $h : \Gamma \longrightarrow \Gamma'$, on désigne par $h^* : \Gamma'^* \longrightarrow \Gamma^*$ l'application duale définie par $h^*(\chi')(\gamma) = \chi'(h(\gamma))$, pour tout $\chi' \in \Gamma'^*$ et $\gamma \in \Gamma$.

1.2 L'application de réciprocité dans le cas modéré

Posons $G = \mathrm{Gal}(k^{(m)}/k^{\mathrm{nr}})$; l'application d'Artin, restreinte à P_T, donne lieu à la suite exacte suivante :

$$1 \longrightarrow E/E_m \longrightarrow k_T^\times/k_m^\times \xrightarrow{\rho} G \longrightarrow 1, \tag{1}$$

dans laquelle $\rho(x) = \left(\frac{k^{(m)}/k}{(x)}\right)$, pour tout $x \in k_T^\times$.

Comme par ailleurs on a la suite exacte canonique :

$$1 \longrightarrow k_m^\times \longrightarrow k_T^\times \xrightarrow{\theta} \prod_{i=1}^{n} \overline{k}_{l_i}^\times \longrightarrow 1,$$

on peut écrire (1) sous la forme :

$$1 \longrightarrow \theta(E) \longrightarrow \prod_{i=1}^{n} \overline{k}_{l_i}^\times \xrightarrow{\pi} G \longrightarrow 1 \tag{2}$$

et on peut considérer π comme une forme particulière de l'application de réciprocité, définie sur le groupe des idèles de k, et restreinte ici aux idèles unités de support T.

On sait que la restriction de π au sous-groupe $\{1\} \times \ldots \times \overline{k}_{l_i}^\times \times \ldots \times \{1\} \simeq \overline{k}_{l_i}^\times$, conduit à la suite exacte :

$$1 \longrightarrow \theta(E_{\frac{m}{l_i}}) \longrightarrow \overline{k}_{l_i}^\times \longrightarrow I_{l_i} \longrightarrow 1. \tag{3}$$

Nous utiliserons également, pour tout $e \geq 1$, les suites exactes suivantes, déduites de (2) :

$$1 \longrightarrow \theta_e(E) \longrightarrow \prod_{i=1}^{n} \overline{k}_{l_i}^\times/\overline{k}_{l_i}^{\times p^e} \xrightarrow{\pi_e} G/G^{p^e} \longrightarrow 1, \tag{4}$$

où θ_e est l'application composée :

$$k_T^\times \xrightarrow{\theta} \prod_{i=1}^{n} \overline{k}_{l_i}^\times \longrightarrow \prod_{i=1}^{n} \overline{k}_{l_i}^\times/\overline{k}_{l_i}^{\times p^e}.$$

1.3 Bases et bases duales

(i) Comme les idéaux premiers $l_i \in T$ vérifient $Nl_i \equiv 1 \bmod p^e$ pour tout $i \in [1,n]$, et que nous aurons à considérer un corps gouvernant extension de $k(\mu_{p^e})$, on peut remplacer les corps résiduels $\overline{k}_{l_i}$ par les corps résiduels $\overline{k(\mu_{p^e})}_{\mathfrak{L}_{i,e}}$, de $k(\mu_{p^e})$ en un idéal premier fixé $\mathfrak{L}_{i,e}$ au-dessus de l_i dans $k(\mu_{p^e})$, puisque les l_i sont totalement décomposés dans $k(\mu_{p^e})/k$. Ainsi, les $\overline{k(\mu_{p^e})}_{\mathfrak{L}_{i,e}}$, notés encore $\overline{k}_{l_i}$, contiennent l'image résiduelle d'une racine primitive p^e-ième de l'unité fixée, ζ_e, ce qui définit une famille cohérente d'éléments d'ordre p^e des groupes $\overline{k}_{l_i}^{\times} = \overline{k(\mu_{p^e})}_{\mathfrak{L}_{i,e}}^{\times}$.

On désigne alors par f_j, $j \in [1,n]$, des générateurs des $\{1\} \times \ldots \times \overline{k}_{l_j}^{\times} \times \ldots \times \{1\}$ tels que [3] :

$$f_j^{\frac{Nl_j-1}{p^e}} = (1, \ldots, \zeta_e \bmod \mathfrak{L}_{j,e}, \ldots, 1)\ , \text{pour tout } j \in [1,n]. \tag{5}$$

On désigne ensuite par $g_{j,e}$ les images canoniques des f_j dans $\prod_{i=1}^{n} \overline{k}_{l_i}^{\times} / \overline{k}_{l_i}^{\times p^e}$.

On associera au choix ci-dessus d'une "base" $(g_{j,e})_{j\in[1,n]}$ de $\prod_{i=1}^{n} \overline{k}_{l_i}^{\times} / \overline{k}_{l_i}^{\times p^e}$, la "base duale" $(g_{j,e}^*)_{j\in[1,n]}$, définie par :

$$g_{j,e}^*(g_{j,e}) = \zeta_e,\ g_{j,e}^*(g_{i,e}) = 1 \text{ pour tout } i \neq j. \tag{6}$$

(ii) On pose $\zeta_1 = \zeta_e^{p^{e-1}}$ et, pour tout $j \in [1,n]$, on note $\mathfrak{L}_{j,1}$ l'idéal premier en-dessous de $\mathfrak{L}_{j,e}$ dans $k(\mu_p)$. Alors, on a, de manière cohérente :

$$f_j^{\frac{Nl_j-1}{p}} = (1, \ldots, \zeta_1 \bmod \mathfrak{L}_{j,1}, \ldots, 1),\ \text{pour tout } j \in [1,n], \tag{7}$$

et si les $g_{j,1}$ sont les images canoniques des f_j dans $\prod_{i=1}^{n} \overline{k}_{l_i}^{\times} / \overline{k}_{l_i}^{\times p}$, les bases duales correspondantes $(g_{j,e}^*)_{j\in[1,n]}$ et $(g_{j,1}^*)_{j\in[1,n]}$ vérifient :

$$g_{j,e}^{*p^{e-1}} = g_{j,1}^*,\ \text{pour tout } j \in [1,n]. \tag{8}$$

Remarque 1.1 *Pour éviter un surcroît de notations, nous confondons les groupes de Galois de la théorie du corps de classes et les groupes de classes correspondants, étant entendu que l'on passe toujours des uns aux autres par une application déduite canoniquement de celle d'Artin.*

[3] Les f_j peuvent être représentés par des éléments de k.

2 Caractérisation des extensions cycliques T-totalement ramifiées de degré p

Dans ce paragraphe, nous résolvons le cas $e = 1$ qui représente une étape particulière pour le cas général.

Soient T et m fixés comme dans (1.1), (ii), soit $G = \mathrm{Gal}(k^{(m)}/k^{\mathrm{nr}})$ et soit L la sous-extension (p-élémentaire) de $k^{(m)}/k^{\mathrm{nr}}$ fixe par $H = G \cap Cl_m^p$.

On a le schéma suivant :

$$\begin{array}{ccccccc} k^{\mathrm{nr}} & \overset{p}{\text{———}} & K_1 & \overset{N}{\text{———}} & L & \overset{H}{\text{———}} & k^{(m)} \\ | & & | & & | & & \\ k^{\mathrm{nr}}[p] & \text{———} & & \text{———} & k^{(m)}[p] & & \\ | & & | & & | & & \\ k & \text{———} & k_1 & \text{———} & M & & \end{array} \tag{9}$$

dans lequel $k^{(m)}[p]$ est le sous-corps de $k^{(m)}$ fixe par Cl_m^p, $k^{\mathrm{nr}}[p] = k^{\mathrm{nr}} \cap k^{(m)}[p]$ est fixe par GCl_m^p ; ainsi L est le composé direct, sur $k^{\mathrm{nr}}[p]$, de k^{nr} et $k^{(m)}[p]$, et comme $\mathrm{Gal}(k^{(m)}[p]/k)$ est un $\mathbb{F}_p$-espace vectoriel, il existe $M \subseteq k^{(m)}[p]$ tel que $k^{(m)}[p]$ soit le composé direct de M et $k^{\mathrm{nr}}[p]$, donc tel que L soit le composé direct, sur k, de M et k^{nr} (on notera que $k^{(m)}[p]$ (resp. $k^{\mathrm{nr}}[p]$) est la sous-extension maximale p-élémentaire de $k^{(m)}$ (resp. k^{nr})).

Donnons tout d'abord des conditions nécessaires :

S'il existe une extension k_1, cyclique de degré p de k, T-totalement ramifiée, $K_1 = k_1 k^{\mathrm{nr}}$ est contenue dans L et on a les faits suivants :

$$N = \mathrm{Gal}(L/K_1) \text{ est un hyperplan du } \mathbb{F}_p\text{-espace vectoriel } G/H \ ; \tag{10}$$

$$G/H = N \oplus I_{l_i} H/H, \text{ pour tout } i \in [1, n]. \tag{11}$$

En effet, (10) est évident et (11) résulte du fait que $I_{l_i} H/H$, qui est le groupe d'inertie de l_i dans L/k^{nr}, est cyclique, d'ordre p, et n'est pas contenu dans N puisque k_1/k, donc K_1/k^{nr}, est totalement ramifiée en l_i.

Montrons que ces conditions sont suffisantes :

S'il existe un hyperplan N de G/H tel que la condition (11) soit vérifiée, alors nécessairement la sous-extension K_1/k^{nr} fixe par N est, pour tout $i \in [1, n]$, totalement ramifiée en l_i ; elle est donc T-totalement ramifiée. Comme L est le composé

direct, sur k, de k^{nr} et M, K_1 se redescend en une extension $k_1 \subseteq M$ de k, cyclique de degré p et T-totalement ramifiée.

On a donc obtenu l'équivalence suivante :

Il existe une sous-extension de $k^{(m)}/k$, cyclique de degré p, T-totalement ramifiée, si et seulement si il existe un hyperplan N de G/H tel que :

$$G/H = N \oplus I_{l_i}H/H, \text{ pour tout } i \in [1,n]. \tag{12}$$

Nous allons traduire (12) en termes d'invariants numériques du corps k ; pour cela nous utilisons la suite exacte générale suivante (cf. [3, § 1.1.1]) :

$$1 \longrightarrow \theta_1(A_T) \longrightarrow \prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p} \xrightarrow{\tilde{\pi}_1} G/H \longrightarrow 1, \tag{13}$$

où $\tilde{\pi}_1$ est le composé surjectif :

$$\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p} \xrightarrow{\pi_1} G/G^p \longrightarrow G/H$$

(cf. (4) pour $e = 1$).

On utilisera notamment la suite exacte duale :

$$1 \longrightarrow (G/H)^* \xrightarrow{\tilde{\pi}_1^*} (\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p})^* \longrightarrow (\theta_1(A_T))^* \longrightarrow 1. \tag{14}$$

D'après (3) et (13), on a, pour tout $i \in [1,n]$ (cf. § (1.3)) :

$$< \tilde{\pi}_1(g_{i,1}) >= I_{l_i}H/H. \tag{15}$$

Alors, de (12), (14) et (15), on déduit l'équivalence des assertions suivantes :

- Il existe un hyperplan N de G/H tel que :

$$G/H = N \oplus I_{l_i}H/H, \text{pour tout } i \in [1,n] \text{ ;}$$

- il existe un hyperplan N de G/H tel que :

$$G/H = N \oplus < \tilde{\pi}_1(g_{i,1}) >, \text{pour tout } i \in [1,n] \text{ ;}$$

- il existe $\chi_1 \in (G/H)^*$ tel que :

$$\chi_1(\tilde{\pi}_1(g_{i,1})) \neq 1, \text{pour tout } i \in [1,n] \text{ ;}$$

- il existe $\chi_1 \in (G/H)^*$ tel que :

$$\tilde{\pi}_1^*(\chi_1)(g_{i,1}) \neq 1, \text{pour tout } i \in [1,n] \text{ ;}$$

- il existe $\varphi_1 \in (\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p})^*$ tel que :

$$\varphi_1 \in \mathrm{Im}(\tilde{\pi}_1^*) \text{ et } \varphi_1(g_{i,1}) \neq 1, \text{pour tout } i \in [1,n] \text{ ;}$$

- il existe $\varphi_1 = \prod_{i=1}^{n} g_{i,1}^{*a_i}$, $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^{\times})^n$ tel que :

$$\theta_1(A_T) \subseteq \mathrm{Ker}(\varphi_1) \text{ (cf. (14))}.$$

La traduction de (12) en termes d'invariants numériques de k est donc :

Il existe $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^{\times})^n$ tel que :

$$\sum_{i=1}^{n} a_i x_i = 0, \text{ pour tout } (x_i)_{i\in[1,n]} \in (\mathbb{Z}/p\mathbb{Z})^n \text{ tel que } \prod_{i=1}^{n} g_{i,1}^{x_i} \in \theta_1(A_T). \qquad (16)$$

3 Existence d'un corps gouvernant (cas $e = 1$)

Nous allons traduire la condition (16) précédente en termes de Frobenius dans un corps gouvernant (i.e. une extension de k qui ne dépende que de k).

Définition 3.1 *On pose* $F_1 = k(\mu_p, A^{\frac{1}{p}})$, *où* $A = \{\alpha \in k^{\times}, (\alpha)$ *puissance p-ième d'idéal* $\}$.

D'après l'égalité $A = A_T k^{\times p}$, on a aussi $F_1 = k(\mu_p, A_T^{\frac{1}{p}})$ mais il est important de noter que F_1 ne dépend que de k.

On rappelle que les choix précisés en (1.3) supposent qu'on a fixé des idéaux $\mathfrak{L}_{i,1}|l_i$, $i \in [1,n]$, du corps $k(\mu_p)$.

La théorie de Kummer montre facilement que $F_1/k(\mu_p)$ est au plus ramifiée en p. Donc pour chaque $i \in [1,n]$, l'idéal premier $\mathfrak{L}_{i,1}$ de $k(\mu_p)$ au-dessus de l_i définit le Frobenius $\sigma_i = (\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}})$, élément de $\mathrm{Gal}(F_1/k(\mu_p))$.

On a alors, pour tout $\alpha \in A_T$ et tout $i \in [1,n]$:

$$\frac{\sigma_i(\alpha^{\frac{1}{p}})}{\alpha^{\frac{1}{p}}} = \zeta_{\alpha,i} \in \mu_p, \tag{17}$$

et, comme par définition :

$$\sigma_i(\alpha^{\frac{1}{p}}) \equiv (\alpha^{\frac{1}{p}})^{Nl_i} \bmod \mathfrak{L}_{i,1},^4$$

il vient :

$$\zeta_{\alpha,i} \equiv \alpha^{\frac{Nl_i-1}{p}} \bmod \mathfrak{L}_{i,1}. \tag{18}$$

Si $\theta_1(\alpha) = \prod_{i=1}^{n} g_{i,1}^{x_{\alpha,i}}$, $x_{\alpha,i} \in \mathbb{Z}/p\mathbb{Z}$, alors (cf. (5) pour $e=1$) :

$$\alpha^{\frac{Nl_i-1}{p}} \equiv \zeta_1^{x_{\alpha,i}} \bmod \mathfrak{L}_{i,1}, \text{ pour tout } i \in [1,n],$$

d'où, par (18) :

$$\zeta_{\alpha,i} = \zeta_1^{x_{\alpha,i}}, \text{ pour tout } i \in [1,n]. \tag{19}$$

La condition (16) est donc équivalente, d'après (19), à :

Il existe $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^n$ tel que :

$$\prod_{i=1}^{n} \zeta_{\alpha,i}^{a_i} = 1, \text{ pour tout } \alpha \in A_T,$$

elle-même équivalente, d'après (17), à :

$$\text{Il existe } (a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^n \text{ tel que } \prod_{i=1}^{n} \sigma_i^{a_i} = 1. \tag{20}$$

On a donc obtenu le résultat suivant :

Proposition 3.1 *(cas $e=1$) : Soit k un corps de nombres et soit $A = \{\alpha \in k^\times, (\alpha)$ puissance p-ième d'idéal $\}$.*

Soit $T = \{l_1, \ldots, l_n\}$ un ensemble de $n \geq 1$ idéaux premiers de k tels que $Nl_i \equiv 1 \bmod p$, pour tout $i \in [1,n]$.

Alors il existe une extension cyclique de degré p sur k, T-totalement ramifiée, si et seulement si il existe $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^n$ tel que :

$$\prod_{i=1}^{n} \left(\frac{k(\mu_p, A^{\frac{1}{p}})/k(\mu_p)}{\mathfrak{L}_{i,1}} \right)^{a_i} = 1.$$

[4] On devrait écrire cette congruence modulo un idéal premier de F_1 au-dessus de $\mathfrak{L}_{i,1}$, mais on vérifie qu'elle vaut pour tout tel idéal, donc modulo l'étendu de $\mathfrak{L}_{i,1}$ dans F_1.

Remarque 3.1 *La condition (20) est indépendante du choix de* $\left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}}\right)$ *(i.e. de* $\mathfrak{L}_{i,1}|l_i$*), mais non le n-uple* $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^n$ *: en effet, si*

$$\omega_1 : \mathrm{Gal}(k(\mu_p)/k) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

désigne le caractère de l'action de $\mathrm{Gal}(k(\mu_p)/k)$ *sur* μ_p *et si pour chaque* $\mathfrak{L}_{i,1}$, $\mathfrak{L}_{i,1}^{s_i}$ *est l'un de ses conjugués,* s_i *étant un élément de* $\mathrm{Gal}(k(\mu_p)/k)$*, alors on sait par la dualité de Kummer (compte tenu du fait que* $\mathrm{Gal}(k(\mu_p)/k)$ *opère trivialement sur le radical A) que :*

$$\left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}^{s_i}}\right) = \left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}}\right)^{\omega_1(s_i)}, \text{ pour tout } i \in [1,n] ;$$

et donc on a :

$$\prod_{i=1}^{n} \left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}}\right)^{a_i} = 1,\ (a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^n,$$

qui est équivalent à :

$$\prod_{i=1}^{n} \left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}^{s_i}}\right)^{a_i\omega_1^{-1}(s_i)} = 1,\ (a_i\omega_1^{-1}(s_i))_{i\in[1,n]} \in ((\mathbb{Z}/p\mathbb{Z})^\times)^n.$$

4 Résolution du cas général

On suppose donc maintenant $e \geq 2$ et on considère un ensemble T formé de $n \geq 1$ idéaux premiers l_i tels que $Nl_i \equiv 1 \bmod p^e$, pour tout $i \in [1,n]$.

On a alors le résultat préliminaire suivant :

Lemme 4.1 *Il existe une extension cyclique* k_e *de* k*, de degré* p^e*,* T*-totalement ramifiée, si et seulement si il existe une extension* k_1 *de* k*, de degré* p*,* T*-totalement ramifiée, telle que* $K_1 = k_1k^{\mathrm{nr}}$ *soit contenue dans une sous-extension cyclique* K_e *de degré* p^e *de* $k^{(m)}/k^{\mathrm{nr}}$*.*

Démonstration :

Un sens étant évident, soit K_e/k^{nr}, cyclique de degré p^e, contenant $K_1 = k_1k^{\mathrm{nr}}$, où k_1/k est T-totalement ramifiée de degré p ; de ce fait, K_1/k^{nr} est aussi T-totalement ramifiée, ce qui entraîne cette propriété pour K_e/k^{nr} car elle est cyclique de degré puissance d'un nombre premier.

Ensuite, en posant $\Gamma_e = \mathrm{Gal}(K_e/k)$, $C_e = \mathrm{Gal}(K_e/k^{\mathrm{nr}})$, on a [5] :

$$\mathrm{rg}_p(\Gamma_e) = \mathrm{rg}_p(\Gamma_e/C_e^{p^{e-1}})(\text{car } e \geq 2) = \mathrm{rg}_p(\mathrm{Gal}(K_1/k)) = \mathrm{rg}_p(\Gamma_e/C_e) + 1,$$

[5] Où $\mathrm{rg}_p(\Gamma)$ désigne $\dim_{\mathbb{F}_p}(\Gamma/\Gamma^p)$ pour tout groupe abélien fini Γ.

puisque k_1 n'est pas contenu dans k^{nr} ; donc C_e est facteur direct dans Γ_e et il existe une extension cyclique k_e de k, de degré p^e, et linéairement disjointe de k^{nr}/k ; comme K_e/k_e est non ramifiée, k_e/k est T-totalement ramifiée.

Démonstration du théorème principal (1.1) :

Considérons le diagramme commutatif suivant, obtenu à partir de la suite exacte (4) du § (1.2) :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (G/G^{p^e})^* & \xrightarrow{\pi_e^*} & \left(\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p^e}\right)^* & \longrightarrow & \theta_e(E)^* & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & (G/G^{p})^* & \xrightarrow{\pi_1^*} & \left(\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p}\right)^* & \longrightarrow & \theta_1(E)^* & \longrightarrow & 1. \end{array}$$

La première condition d'existence de k_e est celle de k_1 (lemme (4.1)), donc l'existence de $\varphi_1 \in (\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p})^*$ vérifiant les conditions suivantes (où l'on rappelle que $H = G \cap Cl_m^p$) (cf. § 2) :

$$\varphi_1 = \tilde{\pi}_1^*(\chi_1),\ \chi_1 \in (G/H)^*, \text{ et } \varphi_1 = \prod_{i=1}^{n} g_{i,1}^{*b_i}, \tag{21}$$

$b_i \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ pour tout $i \in [1, n]$, où l'on rappelle que $\tilde{\pi}_1^*$ est le composé :

$$(G/H)^* \hookrightarrow (G/G^p)^* \overset{\pi_1^*}{\hookrightarrow} \left(\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p}\right)^* ;$$

le noyau N de χ_1 fixe par définition le corps K_1, et l'existence de K_e (cf. lemme (4.1)) est donc équivalente à la condition supplémentaire :

$$\chi_1 = \chi_e^{p^{e-1}},$$

pour $\chi_e \in (G/G^{p^e})^*$, dont le noyau définit K_e.

On a donc, en voyant χ_1 comme caractère de G/G^{p^e} (au lieu de G/H) :

$$\pi_e^*(\chi_1) = \pi_e^*(\chi_e)^{p^{e-1}},$$

soit (puisque l'on a alors $\varphi_1 = \pi_1^*(\chi_1) = \pi_e^*(\chi_1)$) :

$$\varphi_1 = \pi_e^*(\chi_e)^{p^{e-1}} = \varphi_e^{p^{e-1}},$$

où l'on a posé :

$$\varphi_e = \pi_e^*(\chi_e) \in \left(\prod_{i=1}^{n} \overline{k}_{l_i}^{\times}/\overline{k}_{l_i}^{\times p^e}\right)^*.$$

On a donc obtenu, comme condition nécessaire et suffisante d'existence de K_e :

Il existe $\varphi_e \in \mathrm{Im}(\pi_e^*)$ tel que :

$$\varphi_1 = \varphi_e^{p^{e-1}} \in \mathrm{Im}(\tilde{\pi}_1^*) \text{ et } \varphi_1 = \prod_{i=1}^{n} g_{i,1}^{*b_i},\ b_i \in (\mathbb{Z}/p\mathbb{Z})^\times \text{ pour tout } i \in [1,n]$$

$\Longleftrightarrow$ Il existe $\varphi_e = \prod_{i=1}^{n} g_{i,e}^{*a_i}$, $a_i \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ pour tout $i \in [1,n]$ [6] , tel que :

$$\theta_e(E) \subseteq \mathrm{Ker}(\varphi_e) \text{ et } \theta_1(A_T) \subseteq \mathrm{Ker}(\varphi_e^{p^{e-1}})$$

$\Longleftrightarrow$ Il existe $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p^e\mathbb{Z})^\times)^n$ vérifiant les 2 conditions suivantes :

(i) $\sum_{i=1}^{n} a_i y_i \equiv 0 \bmod p$, pour tout $(y_i)_{i\in[1,n]} \in (\mathbb{Z}/p\mathbb{Z})^n$ tel que $\prod_{i=1}^{n} g_{i,1}^{y_i} \in \theta_1(A_T)$,

(ii) $\sum_{i=1}^{n} a_i x_i \equiv 0 \bmod p^e$, pour tout $(x_i)_{i\in[1,n]} \in (\mathbb{Z}/p^e\mathbb{Z})^n$ tel que $\prod_{i=1}^{n} g_{i,e}^{x_i} \in \theta_e(E)$.

Rappelons que les familles $(g_{i,1})_{i\in[1,n]}$ et $(g_{i,e})_{i\in[1,n]}$ dépendent du choix d'idéaux premiers $\mathfrak{L}_{i,1}$ de $k(\mu_p)$ et $\mathfrak{L}_{i,e}$ de $k(\mu_{p^e})$, au-dessus des l_i, avec $\mathfrak{L}_{i,e}|\mathfrak{L}_{i,1}$ (cf. (1.3),(ii)).

On a déjà montré (cf. (20)) que la condition (i) est équivalente à :

$$\prod_{i=1}^{n} \sigma_i^{a_i \bmod p} = 1, \tag{22}$$

où σ_i est le Frobenius de $\mathfrak{L}_{i,1}$ dans $k(\mu_p, A^{\frac{1}{p}})/k(\mu_p)$.

On utilise maintenant le corps gouvernant :

$$F_e = k(\mu_{p^e}, E^{\frac{1}{p^e}}).$$

Si pour tout $i \in [1,n]$, τ_i désigne le Frobenius de $\mathfrak{L}_{i,e}$ dans $\mathrm{Gal}(F_e/k(\mu_{p^e}))$, on a alors pour tout $\varepsilon \in E$:

$$\frac{\tau_i(\varepsilon^{\frac{1}{p^e}})}{\varepsilon^{\frac{1}{p^e}}} = \zeta_{\varepsilon,i} \in \mu_{p^e},$$

puis :

$$\frac{\tau_i(\varepsilon^{\frac{1}{p^e}})}{\varepsilon^{\frac{1}{p^e}}} \equiv \varepsilon^{\frac{Nl_i-1}{p^e}} \bmod \mathfrak{L}_{i,e},$$

ce qui conduit, comme pour le cas $e = 1$, à :

$$\zeta_{\varepsilon,i} = \zeta_e^{x_{\varepsilon,i}},$$

[6] Il est clair que l'on a $a_i \equiv b_i \bmod p$, pour tout $i \in [1,n]$, en vertu de la relation (8).

où $\theta_e(\varepsilon) = \prod_{i=1}^{n} g_{i,e}^{x_{e,i}}$, $x_{e,i} \in \mathbb{Z}/p^e\mathbb{Z}$.

La condition (ii) précédente est donc équivalente à :

$$\prod_{i=1}^{n} \zeta_{e,i}^{a_i} = 1, \text{ pour tout } \varepsilon \in E,$$

qui est bien équivalente à :

$$\prod_{i=1}^{n} \tau_i^{a_i} = 1. \tag{23}$$

Notons que le n-uple $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p^e\mathbb{Z})^\times)^n$ dépend du choix des idéaux premiers $\mathfrak{L}_{i,e}$ dans $k(\mu_{p^e})$ mais non les conditions (22) et (23). En effet, si

$$\omega_e : \mathrm{Gal}(k(\mu_{p^e})/k) \longrightarrow (\mathbb{Z}/p^e\mathbb{Z})^\times$$

désigne le caractère de l'action de $\mathrm{Gal}(k(\mu_{p^e})/k)$ sur μ_{p^e}, si pour chaque $\mathfrak{L}_{i,e}$, $\mathfrak{L}_{i,e}^{t_i'}$ est l'un de ses conjugués, t_i' étant un élément de $\mathrm{Gal}(k(\mu_{p^e})/k)$, si $\mathfrak{L}_{i,1}$ est l'idéal premier de $k(\mu_p)$ au-dessous de $\mathfrak{L}_{i,e}$, alors pour tout $i \in [1,n]$, l'idéal premier de $k(\mu_p)$ au-dessous de $\mathfrak{L}_{i,e}^{t_i'}$ est $\mathfrak{L}_{i,1}^{t_i}$, où t_i est la restriction de t_i' à $k(\mu_p)$ et on a :

$$\omega_e(t_i') \equiv \omega_1(t_i) \bmod p,$$

et par la dualité de Kummer, on a, pour tout $i \in [1,n]$:

$$\begin{aligned}
\left(\frac{F_e/k(\mu_{p^e})}{\mathfrak{L}_{i,e}^{t_i'}}\right) &= \left(\frac{F_e/k(\mu_{p^e})}{\mathfrak{L}_{i,e}}\right)^{\omega_e(t_i')} \\
\left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}^{t_i}}\right) &= \left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}}\right)^{\omega_1(t_i)} ;
\end{aligned}$$

donc on peut écrire que :

$$\prod_{i=1}^{n} \left(\frac{F_e/k(\mu_{p^e})}{\mathfrak{L}_{i,e}}\right)^{a_i} = 1 \text{ et } \prod_{i=1}^{n} \left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}}\right)^{a_i \bmod p} = 1, \ (a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p^e\mathbb{Z})^\times)^n,$$

est équivalent à :

$$\prod_{i=1}^{n} \left(\frac{F_e/k(\mu_{p^e})}{\mathfrak{L}_{i,e}^{t_i'}}\right)^{a_i\omega_e^{-1}(t_i')} = 1 \text{ et } \prod_{i=1}^{n} \left(\frac{F_1/k(\mu_p)}{\mathfrak{L}_{i,1}^{t_i}}\right)^{a_i\omega_e^{-1}(t_i) \bmod p} = 1,$$

avec $(a_i\omega_e^{-1}(t_i))_{i\in[1,n]} \in ((\mathbb{Z}/p^e\mathbb{Z})^\times)^n$.

On a donc obtenu que l'existence de k_e est équivalente à celle de $(a_i)_{i\in[1,n]} \in ((\mathbb{Z}/p^e\mathbb{Z})^\times)^n$ satisfaisant aux deux conditions suivantes :

$$\text{(i)} \prod_{i=1}^{n} \left(\frac{k(\mu_p, A^{\frac{1}{p}})/k(\mu_p)}{\mathfrak{L}_{i,1}} \right)^{a_i \bmod p} = 1,$$

$$\text{(ii)} \prod_{i=1}^{n} \left(\frac{k(\mu_{p^e}, E^{\frac{1}{p^e}})/k(\mu_{p^e})}{\mathfrak{L}_{i,e}} \right)^{a_i} = 1 \text{ (si } e \geq 2).$$

On remarque alors que la condition (i) précédente s'écrit aussi :

$$\prod_{i=1}^{n} \left(\frac{k(\mu_{p^e}, (A^{p^{e-1}})^{\frac{1}{p^e}})/k(\mu_{p^e})}{\mathfrak{L}_{i,e}} \right)^{a_i} = 1,$$

puisque les l_i sont totalement décomposés dans $k(\mu_{p^e})$; la condition (ii) étant inchangée dans l'extension $k(\mu_{p^e}, E^{\frac{1}{p^e}})/k(\mu_{p^e})$, le résultat découle de la considération de l'extension composée $k(\mu_{p^e}, (EA^{p^{e-1}})^{\frac{1}{p^e}})/k(\mu_{p^e})$.

Et le théorème principal est démontré.

5 Remarques, exemples et compléments

Remarque 5.1 *Dans [2], il était demandé, pour construire une extension cyclique k_e de k , de degré p^e, T-totalement ramifiée, que pour chaque $l \in T$, les images résiduelles $\overline{A}_T$ et $\overline{E}$ de A_T et E dans $\overline{k}_l$ vérifient :*

$$\overline{A}_T \subseteq \overline{k}_l^{\times p} \text{ et } \overline{E} \subseteq \overline{k}_l^{\times p^e},$$

c'est-à-dire que les conditions du théorème soient vérifiées pour chaque singleton $\{l\}$, $l \in T$.

Le théorème (1.1) permet donc d'élargir considérablement l'éventail des ensembles T conduisant à une solution, dès que $|T| \geq 2$. Nous allons illustrer ce fait au moyen d'un exemple numérique.

Exemple : Soit $k = \mathbb{Q}(\sqrt{10})$ et soit $p = 2$. On a :

$$\begin{aligned} E &= < -1, \varepsilon = 3 + \sqrt{10} >, \\ A &= < -1, \varepsilon = 3 + \sqrt{10}, \eta = 1 + \sqrt{10} > k^{\times 2}. \end{aligned}$$

On recherche les ensembles d'idéaux premiers impairs T à deux éléments.

(α) ($e = 1$). Il existe une extension quadratique k_1 de k, T-totalement ramifiée, si et seulement si l_1 et l_2 sont tels que :

$$\left(\frac{k(\sqrt{A})/k}{l_1} \right) = \left(\frac{k(\sqrt{A})/k}{l_2} \right).$$

On vérifie que cela donne les huit possibilités suivantes [7] :

$$\left(\frac{\varepsilon}{l_1}\right)_2 = \left(\frac{\varepsilon}{l_2}\right)_2,\ \left(\frac{\eta}{l_1}\right)_2 = \left(\frac{\eta}{l_2}\right)_2,\ Nl_1 \equiv Nl_2 \bmod 4,$$

où $\left(\frac{\cdot}{l_1}\right)_2$, $\left(\frac{\cdot}{l_2}\right)_2$ sont les symboles de restes quadratiques modulo l_1 et l_2 dans les corps résiduels.

(β) ($e = 2$). Il existe une extension cyclique k_2 de k de degré 4, T-totalement ramifiée, si et seulement si l_1 et l_2 vérifient les trois conditions suivantes :

(i) $Nl_1 \equiv Nl_2 \equiv 1 \bmod 4$,

(ii) $\left(\frac{k(\sqrt{A})/k}{l_1}\right) = \left(\frac{k(\sqrt{A})/k}{l_2}\right)$,

(iii) $\left(\frac{k(\sqrt{-1},\sqrt[4]{E})/k(\sqrt{-1})}{\mathfrak{L}_{1,2}}\right) = \left(\frac{k(\sqrt{-1},\sqrt[4]{E})/k(\sqrt{-1})}{\mathfrak{L}_{2,2}}\right)^{\pm 1}$, $\mathfrak{L}_{i,2}|l_i$, $i = 1, 2$.

La condition (iii) conduit aux six possibilités suivantes (sous la condition (i)) :

$$\left(\frac{\varepsilon}{l_1}\right)_4 = \left(\frac{\varepsilon}{l_2}\right)_4^{\pm 1},\ Nl_1 \equiv Nl_2 \bmod 8,$$

où $\left(\frac{\cdot}{l_1}\right)_4$, $\left(\frac{\cdot}{l_2}\right)_4$ sont les symboles de restes de puissances 4-ièmes, modulo l_1 et l_2 dans les corps résiduels.

Il en résulte qu'il existe une extension cyclique de degré 4 de k, T-totalement ramifiée, dans chacune des douze situations suivantes (toujours sous la condition nécessaire (i) et compte tenu de la note de bas de page) :

$$\left(\frac{\varepsilon}{l_1}\right)_4 = \left(\frac{\varepsilon}{l_2}\right)_4^{\pm 1},\ \left(\frac{\eta}{l_1}\right)_2 = \left(\frac{\eta}{l_2}\right)_2,\ Nl_1 \equiv Nl_2 \bmod 8.$$

Le cas $\left(\frac{\varepsilon}{l_1}\right)_4 = \left(\frac{\varepsilon}{l_2}\right)_4 = \left(\frac{\eta}{l_1}\right)_2 = \left(\frac{\eta}{l_2}\right)_2 = 1$, $Nl_1 \equiv Nl_2 \bmod 8$, est équivalent à $\overline{A}_T \subseteq \overline{k}_{l_i}^{\times 2}$ et $\overline{E} \subseteq \overline{k}_{l_i}^{\times 4}$, pour $i = 1, 2$, et constitue le seul cas envisagé dans [2] pour le degré 4.

Or on peut vérifier que si $T = \{l_1, l_2\}$, avec $l_1 = \mathfrak{p}_{41}$ (idéal premier de k au-dessus de 41) et $l_2 = (7)$, ε et η ne sont pas des carrés modulo l_1 et l_2 ; ceci donne l'existence d'une extension quartique cyclique de k, T-totalement ramifiée, tandis qu'il n'existe aucune extension quadratique de k, $\{\mathfrak{p}_{41}\}$-totalement ramifiée, ou $\{(7)\}$-totalement ramifiée.

[7] Si T contient un idéal premier au-dessus de 3, on doit, dans les écritures ci-après, remplacer η par η' étranger à 3.

Remarque 5.2 *Revenons à l'énoncé général du théorème (1.1) ; comme l'extension* $k(\mu_{p^e}, (EA^{p^{e-1}})^{\frac{1}{p^e}})/k(\mu_{p^e})$ *est au plus ramifiée au-dessus de* $p\infty$*, son conducteur* $\mathfrak{f}$ *peut se calculer facilement, et permet de ramener le problème de la recherche des ensembles* T *à des calculs dans le groupe des classes généralisées* $Cl_{\mathfrak{f}}$ *de* $k(\mu_{p^e})$*.*

En effet, à partir de toute relation de la forme :

$$\prod_{i=1}^{n} \sigma_i^{a_i} = 1 \ , a_i \not\equiv 0 \bmod p,$$

sur des éléments de $\mathrm{Gal}(k(\mu_{p^e}, (EA^{p^{e-1}})^{\frac{1}{p^e}})/k(\mu_{p^e}))$*, il suffit, par le corps de classes sur* $k(\mu_{p^e})$*, de choisir, pour chaque* i*, un idéal premier* $\mathfrak{L}_{i,e}$ *de* $k(\mu_{p^e})$*, totalement décomposé dans* $k(\mu_{p^e})/k$*, dont la classe généralisée corresponde, par l'application d'Artin, à l'élément* σ_i *; un ensemble* T *est alors formé des* n *idéaux premiers* l_i *de* k *en-dessous des* $\mathfrak{L}_{i,e}$*.*

Le théorème de Čebotarev conduit au fait qu'il y a une infinité (dont la densité pourrait être précisée) d'ensembles T *(à* n *fixé) conduisant à des extensions cycliques* T*-totalement ramifiées de degré* p^e *de* k*.*

On peut, avec les techniques précédentes, généraliser le théorème (1.1) dans différentes directions ; par exemple ($p \neq 2$) : Soit $T = T_1 \cup \ldots \cup T_e$ une réunion disjointe d'ensembles de places modérées ($T_1 \neq \emptyset$) telles que $Nl \equiv 1 \bmod p^{e_l}$, avec $e_l \geq e - r + 1$ pour tout $l \in T_r$; alors il existe une extension cyclique T-ramifiée de degré p^e de k, pour laquelle l'indice de ramification de tout $l \in T_r$ est égal à p^{e-r+1}, $1 \leq r \leq e$, si et seulement si il existe une relation de la forme :

$$\prod_{r=1}^{e} \prod_{l \in T_r} \left(\frac{k(\mu_{p^e}, (EA^{p^{e-1}})^{\frac{1}{p^e}})/k(\mu_{p^e})}{\mathfrak{L}_e} \right)^{a_l \, \mathrm{Min}(p^{e_l - e + r - 1}, p^{r-1})} = 1,$$

avec $\mathfrak{L}_e | l$ dans $k(\mu_{p^e})/k$ et $a_l \not\equiv 0 \bmod p$, pour tout $l \in T$.

Le cas $p = 2$ est analogue mais exige une formulation différente en raison de la possibilité d'imposer ou non la complexification de places à l'infini, également modérées.

On peut enfin caractériser facilement les extensions cycliques de degré p de k^{nr}, modérément ramifiées, abéliennes sur k, non décomposées sur k.

Références

[1] Cornell, G., The structure of the ray class group, In : *Algebraic Number Theory*, RIMS, Kokyuroku, 1987.

[2] Gras, G., Principalisation d'idéaux par extensions absolument abéliennes, *Jour. Number Theory*, 62, 2 (1997), 403-421.

[3] Maire, C., *Extensions T-ramifiées modérées S-décomposées*, Thèse de Doctorat, Université de Franche-Comté Besançon, 1995.

[4] Stevenhagen, P., *Ray class groups and governing fields*, Ph. D. Thesis, University of Amsterdam, 1988.

Summary :

Let k be a number field and p^e, $e \geq 1$, a prime power. We give a very simple governing field for the solution of the following problem : characterize all the sets T of primes of k, not dividing p, for which there exists a cyclic extension of degree p^e of k, unramified outside T, and totally ramified at all places of T.

Key words :

governing fields ; T-ramified extensions ; class field theory

Georges Gras
U.F.R. Sciences
Laboratoire de Mathématiques
UMR 6623 au CNRS
F-25030 Besançon cedex

Adeline Munnier
U.F.R. Sciences
Laboratoire de Mathématiques
UMR 6623 au CNRS
F-25030 Besançon cedex

N.B. Ce texte a été soumis à une revue de théorie des nombres en octobre 1997 ; le "Referee" de cette revue n'ayant pas daigné donner un avis durant plus d'un an, il a été retiré pour la présente publication.