

*SUR LA p -RAMIFICATION NON ABELIENNE
DE CORPS DE NOMBRES TOTALEMENT REELS*

SUR LA p -RAMIFICATION NON ABELIENNE DE CORPS
DE NOMBRES TOTALEMENT REELS

NGUYEN QUANG DO Thong

I.— Introduction :

Soient K une extension finie de \mathbb{Q} , p un nombre premier impair, S un ensemble fini de places de K contenant les places au-dessus de p . Un objet arithmétique important attaché au couple (K, S) est le groupe de Galois G_S de la pro- p -extension (non abélienne) S -ramifiée maximale de K (voir par exemple l'introduction de [12]). On se propose ici d'étudier la structure de G_S par analogie avec le groupe fondamental d'une surface de Riemann "percée" d'un nombre fini de "trous". L'analogie du genre est l'invariant λ d'un certain module d'Iwasawa attaché à K . Le cas de genre zéro a été étudié en détail dans [12]. On aborde ici l'étude des cas de genre ≥ 1 . Faute d'une théorie suffisamment développée des fonctions L p -adiques à plusieurs variables, on se limitera la plupart du temps aux corps de nombres totalement réels. Les résultats concerneront principalement les quotients nilpotents $G_S/G_S^{(m)}$.

II.— Rappels de résultats connus :

On adoptera les notations générales suivantes :

K = un corps de nombres algébriques, de degré fini sur \mathbb{Q} .

p = un nombre premier impair fixé.

S_p = l'ensemble des places de K au-dessus de p .

S = un ensemble fini de places de K contenant S_p .

K_S = la pro- p -extension S -ramifiée (i.e. non ramifiée en dehors de S) maximale de K .

$G_S = \text{Gal}(K_S/K) = G_S(K)$.

II.1 Invariants cohomologiques :

Soient

$d = d(G_S) = \dim H^1(G_S, \mathbf{Z}/p\mathbf{Z})$ le nombre minimal de générateurs de G_S ,

$r = r(G_S) = \dim H^2(G_S, \mathbf{Z}/p\mathbf{Z})$ le nombre minimal de relations de G_S .

On sait (voir par exemple [8]) que la dimension cohomologique de G_S est ≤ 2 , et que sa caractéristique d'Euler-Poincaré est donnée par :

$$\chi(G_S) = -1 + d - r = r_2 \quad (= \text{le nombre de places complexes de } K).$$

Pour tout $n \geq 1$, soit $V_S^n = \{x \in K^*; x \in K_v^{*p^n} \forall v \in S, v(x) \equiv 0 \pmod{p^n} \forall v \text{ finie } \notin S\} / K^{*p^n}$.

On a la suite exacte de Poitou-Tate :

$$0 \rightarrow \mu_{p^n}(K) \rightarrow \prod_{v \in S} \mu_{p^n}(K_v) \rightarrow H^2(G_S, \mathbf{Z}/p^n\mathbf{Z})^* \rightarrow V_S^n \rightarrow 0, \quad (1)$$

où $\mu_{p^n}(F)$ désigne le groupes des racines p^n -ièmes de l'unité dans F , et $(.)^*$ le dual de Pontryagin. Cette suite montre que :

- d'une part, $r(G_S) = \sum_{v \in S} \varepsilon(K_v) - \varepsilon(K) + \dim V_S^1$, où $\varepsilon(F) = 1$ (resp. 0) si F contient

(resp. ne contient pas) le groupe μ_p des racines p ièmes de l'unité.

- d'autre part, les relations de G_S se composent des "relations locales" en $v \in S$ (non indépendantes en général, à cause de la formule du produit) et de "relations globales" additionnelles, en nombre égal à $\dim V_S^1$. Ce sont ces relations globales qu'on doit s'efforcer de décrire.

II.2 Corps de classes global :

D'après le corps de classes global (ou d'après 2.1), on sait que G_S^{ab} est un \mathbf{Z}_p -module de type fini, donc se décompose sous la forme d'un produit direct :

$$G_S^{ab} \simeq T_S \times \mathbf{Z}_p^{1+r_2+\delta},$$

où $T_S = T_S(K)$ est le p -groupe de torsion (fini), et δ un entier ≥ 0 , conjecturalement nul (Leopoldt). En termes cohomologiques, la **conjecture de Leopoldt** équivaut à $H^2(G_S, \mathbf{Q}_p/\mathbf{Z}_p) = 0$, ou encore à $H^2(G_S, \mathbf{Z}/p\mathbf{Z})^* \simeq_p T_S$ (= le sous-groupe des éléments d'ordre p de T_S). Si elle est vérifiée, la torsion T_S est décrite par la suite exacte de Poitou-Tate :

$$0 \rightarrow \mu(K) \rightarrow \prod_{v \in S} \mu(K_v) \rightarrow T_S \rightarrow V_S \rightarrow 0, \quad (2)$$

où $V_S = \varinjlim V_S^n$ et $\mu(F)$ désigne le groupe de toutes les racines p^n -ièmes de l'unité contenues dans F (voir par exemple [14]). Une connaissance explicite des relations de G_S (resp. des relations globales additionnelles) permettrait de donner une description explicite de T_S (resp. de V_S), i.e. une "théorie explicite du corps de classes".

II.3 Corps de classes nilpotent :

Soit $G_S^{(i)}$ la suite centrale descendante de G_S , définie par :

$$G_S^{(1)} = G_S, \quad G_S^{(2)} = [G_S, G_S], \dots, G_S^{(i+1)} = [G_S, G_S^{(i)}].$$

De même que l'objet de la théorie (abélienne) du corps de classes est la description de $G_S^{ab} = G_S/G_S^{(2)}$, l'objet de ce qu'on pourrait appeler le **"corps de classes nilpotent"** (de degré 2) serait la description de $G_S/G_S^{(3)}$. Les résultats dans cette direction sont encore peu nombreux. Citons la description de $G_S/G_S^{(3)}$ par générateurs et relations donnée par Fröhlich quand $K = \mathbb{Q}$ ([3]), par Ullom & Watt quand $K = \mathbb{Q}(\mu_p)$, p régulier ([21]), et plus généralement par A. Movahhedi et l'auteur quand K est p -rationnel, i.e. $r(G_{S_p}) = 0$ ([12]). Dans l'hypothèse où $r(G_{S_p}) \neq 0$, citons le cas où K contient μ_p et $\dim V_{S_p}^1 = 0$, étudié par l'auteur ([17]), et le cas où K est un corps quadratique réel tel que $r(G_{S_p}) = \dim V_{S_p}^1 = 1$, étudié par K. Komatsu ([9]) ; voir aussi 3.4 ci-dessous.

II.4 Description de G_S :

Rappelons d'abord les résultats locaux sur lesquels s'appuiera l'étude globale. Soit K_v un corps local v -adique, i.e. une extension finie d'un corps \mathbb{Q}_ℓ ($v \mid \ell$). Posons $n_v = 0$ si $\ell \neq p$, $[K_v : \mathbb{Q}_p]$ si $\ell = p$. La structure du groupe de Galois G_v de la pro- p -extension maximale de G_v est entièrement connue (voir par exemple [19]) : $d(G_v) = n_v + 1 + \varepsilon(K_v)$, $r(G_v) = \varepsilon(K_v)$; si $\varepsilon(K_v) = 1$, i.e. si K_v contient μ_p , G_v peut être décrit par une unique relation, ρ_v , connue explicitement :

- (i) si $v \nmid p$, $\rho_v = \sigma_v^{Nv-1}[\sigma_v, \tau_v]$, où Nv désigne la norme de l'idéal premier associé à la place v , τ_v un générateur du groupe d'inertie (procyclique) et σ_v un relèvement du Frobenius.
- ii) Si $v \mid p$, on peut choisir des générateurs $\sigma_1, \dots, \sigma_{2+n_v}$ de G_v t.q.
 $\rho_v = \sigma_1^{q_v}[\sigma_1, \sigma_2] \cdots [\sigma_{1+n_v}, \sigma_{2+n_v}]$, avec $q_v = \# \mu(K_v)$ (Demuškin).

Dans l'étude globale, il est clair, d'après la théorie du corps de classes, que **l'analogue de $\mu(K_v)$ n'est pas $\mu(K)$, mais le groupe de torsion $T_{S_p}(K)$** . Un premier démarquage de l'étude locale donne les résultats suivants :

a) Le pro- p -groupe $G_{S_p}(K)$ est libre (i.e. $r(G_{S_p}) = 0$) si et seulement si K vérifie la conjecture de Leopoldt en p et $T_{S_p}(K) = 0$. Dans ce cas, le corps K est appelé p -rationnel ([12]).

Exemple : $K = \mathbb{Q}$, ou $K = \mathbb{Q}(\mu_p)$, p régulier.

Si K est p -rationnel, l'ensemble S est appelé **primitif** si les Frobenius en les places modérées ($w \in S - S_p$) engendrent un facteur direct de $G_{S_p}^{ab}$, de rang égal à $|S - S_p|$; dans ce cas, on a un isomorphisme canonique : $G_S \overset{\sim}{\leftarrow} \prod_{w \in S - S_p} * G_S^w * F$, où $*$ désigne le pro- p -produit libre, G_S^w est un groupe de décomposition (défini à conjugaison près) en w , décrit comme dans le cas local i) ci-dessus, et F un pro- p -groupe libre de rang adéquat ([12], 3.3).

b) Si K contient μ_p , le pro- p -groupe $G_S(K)$ est de Demuškin si et seulement si $S = S_p = \{v_1, v_2\}$ et $G_S = G_S^{v_1} = G_S^{v_2}$ (Tsvetkov [20]). Notons que dans ce cas, p est forcément régulier.

Exemple : $p = 3$, $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-26})$. Dans ce cas, G_{S_3} est un pro-3-groupe à 4 générateurs $\sigma_1, \dots, \sigma_4$ et une relation $\sigma_1^3[\sigma_1, \sigma_2] \cdot [\sigma_3, \sigma_4] = 1$.

Si K ne contient pas μ_p , on ne sait pas caractériser le couple (K, S) pour que G_S soit un groupe de Demuškin (voir cependant 4.2 ci-dessous)^(*).

Si K contient μ_p , par comparaison des groupes locaux G_v et des groupes de décomposition G_S^v , Kuz'min [10] a donné une "classification" de G_S suivant la finitude ou non des indices $(G_S : G_S^v)$. Ses résultats ont été repris et complétés par Wingberg [24] et peuvent s'énoncer ainsi ([24], thm. 4 & A) :

Supposons que K contient μ_p . Alors :

c) Si pour $v \in S$, on a $(G_S : G_S^v) = \infty$, alors $G_v \simeq G_S^v$.

d) S'il existe $v \in S$ t.q. $(G_S : G_S^v) < \infty$, alors forcément $v \in S_p$, $G_S = G_S^v$ et l'on a un isomorphisme canonique $G_S \xleftarrow{\sim} \ast_{w \in S - \{v\}} G_w \ast F$, où F est un pro- p -groupe libre de rang adéquat.

e) Si $(G_S : G_S^v) = \infty$ pour tout $v \in S$, alors le pro- p -groupe G_S est de Cohen-Macaulay strict ([19], app.).

Notons que d) contient b), ainsi que a) si $K \supset \mu_p$. A notre connaissance, les propositions a) à e) sont les seuls résultats généraux disponibles sur la structure de $G_S(K)$. Le problème reste à peu près entier, par exemple, dans le cas totalement réel.

^(*) NB : Le problème évoqué vient d'être résolu par K. Wingberg.

III.— Matrice de relations :

Nous adopterons les notations suivantes :

K_∞ = la \mathbf{Z}_p -extension cyclotomique de K , $\Gamma = \text{Gal}(K_\infty/K)$, $H_S = \text{Gal}(K_S/K)$. L'abélianisé H_S^{ab} est un module compact de type fini sur l'algèbre d'Iwasawa $\Lambda = \mathbf{Z}_p[[\Gamma]]$. Son Λ -rang est égal à r_2 ("conjecture faible de Leopoldt" ; voir e.g. [6], [13]).

III.1 Dérivées de Fox :

Soient $d = d(G_S)$, $r = r(G_S)$ (voir 2.1). On choisira un système minimal de générateurs y, x_1, \dots, x_{d-1} de G_S de la façon suivante : y est un relèvement arbitraire d'un générateur topologique γ de Γ , et les x_i engendrent normalement et minimalement H_S (c'est toujours possible, par le lemme de Nakayama). Les images \bar{x}_i des x_i dans H_S^{ab} forment alors un système minimal de Λ -générateurs de H_S^{ab} .

Soit $1 \rightarrow R \rightarrow F \rightarrow G_S \rightarrow 1$ une présentation minimale de G_S par générateurs et relations. On notera (par abus de langage) y, x_1, \dots, x_{d-1} un système minimal de générateurs du pro- p -groupe libre F , et w_1, \dots, w_r un système minimal de générateurs normaux de R . On en déduit une présentation minimale $1 \rightarrow R \rightarrow E \rightarrow H_S \rightarrow 1$, où E est un pro- p -groupe libre sur les conjugués par y des x_i . Par abélianisation, on obtient une suite exacte de Λ -modules ([13], 1.4) :

$$0 \rightarrow \bigoplus_{j=1}^r \Lambda \bar{w}_j \xrightarrow{\varphi} \bigoplus_{i=1}^{d-1} \Lambda \bar{x}_i \rightarrow H_S^{ab} \rightarrow 0 \quad , \quad (3)$$

où les \bar{x}_i (resp. \bar{w}_j) désignent les images des x_i (resp. w_j) dans E^{ab} (resp. $R/[R, E]$) et l'injectivité de φ équivaut à la validité de la conjecture faible de Leopoldt. La matrice \mathcal{R} représentant l'homomorphisme φ est une matrice à $(d-1)$ lignes et r colonnes ; ses coefficients $f_{ij} \in \Lambda$ sont donnés par : $f_{ij} = \left(\overline{\frac{\partial w_j}{\partial x_i}} \right)$, où $\frac{\partial w_j}{\partial x_i}$ désigne la dérivée de Fox dans $\mathbf{Z}_p[[F]]$ et $\left(\overline{\frac{\partial w_j}{\partial x_i}} \right)$ l'image de cette dérivée dans $\mathbf{Z}_p[[\Gamma]]$ (pour des détails, voir [13], 4.1). En résumé, la connaissance des relations w_j permet de décrire complètement, via la "matrice de relations" \mathcal{R} , la structure du Λ -module H_S^{ab} . En particulier, d'après la théorie de Fitting, la série caractéristique d'Iwasawa attachée au sous- Λ -module de torsion de H_S^{ab} est le *p.g.c.d.* des déterminants d'ordre r de \mathcal{R} .

III.2 Description de G_S modulo $G_S^{(k)} \cdot H_S^{(2)}$:

Inversement, supposons connue la matrice de relations $\mathcal{R} = (f_{ij})$, $f_{ij} \in \Lambda$. Par le changement de variables habituel $T = \gamma - 1$, chaque f_{ij} s'écrit comme une série formelle à coefficients dans \mathbf{Z}_p :

$$f_{ij} = \sum_{k=0}^{\infty} \alpha_{ijk} T^k, \quad \alpha_{ijk} \in \mathbf{Z}_p.$$

Proposition III.3 :

Avec les notations précédentes, le pro- p -groupe G_S peut être engendré minimale-ment par d générateurs y, x_1, \dots, x_{d-1} liés par r relations indépendantes w_j telles que, pour tout entier m :

$$w_j \equiv \prod_{i=1}^{d-1} \prod_{k=0}^m [y, x_i]_k^{\alpha_{ijk}} \pmod{G_S^{(m)} \cdot H_S^{(2)}}.$$

(Ici $[y, x]_k$ désigne le commutateur itéré $[y, [y, \dots, [y, x]] \dots]$ (k fois), avec la convention que $[y, x]_0 = x$).

Preuve : En identifiant \bar{w}_j à $\varphi(\bar{w}_j)$, les relations matricielles de la suite exacte (3) de 2.1 s'écrivent en notation additive :

$$\bar{w}_j = \sum_{i=1}^{d-1} f_{ij} \cdot \bar{x}_i = \sum_{i=1}^{d-1} \sum_{k=0}^{\infty} \alpha_{ijk} T^k \cdot \bar{x}_i.$$

Comme $T = \gamma - 1$, $T \cdot \bar{x} = \overline{yx y^{-1} x^{-1}} = \overline{[y, x]}$ en notation multiplicative, d'où la forme des relations w_j donnée dans l'énoncé. \diamond

Corollaire III.4 : (comparer à [9], thm. p. 245)

Supposons que $d = 2$ et $r = 1$ ($\Leftrightarrow K$ est totalement réel et $r = 1$). Alors G_S peut être engendré minimalement par deux générateurs y, x liés par une relation w telle que $w \equiv x^{\alpha_0} [y, x]^{\alpha_1} \pmod{G_S^{(3)}}$, où α_0, α_1 sont les premiers coefficients de la série caractéristique $f(T)$ du Λ -module de torsion H_S^{ab} . En particulier, $\alpha_0 \neq 0$ si et seulement si K vérifie la conjecture de Leopoldt. Si $S = S_p$ et $\alpha_0 \neq 0$, on a : $\alpha_0 \sim \#T_{S_p}(K) \sim \#\mu(K(\mu_p)) \text{ Rés}_{s=1} \zeta_p(K, s)$, où \sim signifie l'égalité à unité p -adique près.

Preuve : Par hypothèse, H_S est engendré par les conjugués d'un seul élément x , d'où $H_S^{(2)} \subset G_S^{(3)}$. La forme de la relation w résulte alors de 3.3.1. Il est bien connu que la conjecture de Leopoldt pour K équivaut à la non-nullité de α_0 . Comme le groupe des co-invariants $(H_S^{ab})_{\Gamma}$ est isomorphe à $\text{Gal}(K_S^{ab}/K_{\infty})$ et comme K est totalement réel, la conjecture de Leopoldt pour K entraîne que $(H_S^{ab})_{\Gamma} \simeq T_S(K)$ et $\alpha_0 \sim \#T_S(K)$ car H_S^{ab} n'a pas de sous- Λ -module fini non nul. Soit $u = \mathcal{K}(\gamma)$, où \mathcal{K} désigne le caractère cyclotomique. En utilisant les théorèmes de Mazur-Wiles [11] et Wiles [23] (ex - "conjecture principale"), qui relie la série caractéristique $f(T)$ à la fonction $\zeta_p(s, K)$, un simple calcul de développement limité (pour des détails, voir [1]) montre que $\alpha_0 \sim (u - 1) \text{ Rés}_{s=1} \zeta_p(s, K)$. Or $u - 1 \sim \#\mu(K(\mu_p))$. \diamond

Exemples : (On prend $S = S_p$).

i) **Corps quadratiques réels :**

Pour tous les corps quadratiques réels $K = \mathbb{Q}(\sqrt{d})$, $d \leq 200$, sans facteur carré, $p = 3$, il résulte des calculs de [4] que $r = 0$ ou 1. Voir aussi le tableau I. Notons que les tables de [7] donnent aussi les premiers coefficients de la série caractéristique.

ii) **Corps cyclotomiques :**

Soit $K = \mathbb{Q}(\mu_p)^+$. Alors $r = 1$ si et seulement si la “partie moins” du p -groupe des classes de $\mathbb{Q}(\mu_p)$ est cyclique (voir la suite exacte (1) de 2.1.).

Dans toute la suite, notre but va être :

- d’expliciter si possible la matrice de relations \mathcal{R} ,
- de nous débarrasser si possible des commutateurs de $H_S^{(2)}$ dans l’écriture des relations (voir 3.3.).

IV.— Genre un :

A partir de maintenant, K est un corps **totale-ment réel** et $S = S_p$. Le module $H_{S_p}^{ab}$ sera noté \mathcal{X}_∞ . Pour simplifier l’exposé, on fera en plus les hypothèses suivantes (qui sont vérifiées par exemple si K est abélien sur \mathbb{Q}) :

- i) Toutes les extensions K_n/K contenues dans la \mathbb{Z}_p -extension cyclotomique K_∞/K vérifient la conjecture de Leopoldt.
- ii) L’invariant μ du module \mathcal{X}_∞ est nul.

L’analogie du genre est l’invariant λ de \mathcal{X}_∞ . Précisons ses liens avec le nombre de relations r de $G_{S_p}(K)$:

Lemme IV.1 : (*voir aussi [16], 2.4*)

- a) *Le nombre minimal de \wedge -générateurs de \mathcal{X}_∞ est égal à r .*
- b) *La suite $r_n = r(G_{S_p}(K_n))$ est croissante et converge vers λ .*

Preuve : a) résulte du lemme de Nakayama (et est indépendant de Leopoldt). Montrons b). Pour tout $n \geq 0$, posons $\Gamma_n = \text{Gal}(K_\infty/K_n)$ et $T_n = T_{S_p}(K_n)$. Comme K_n vérifie la conjecture de Leopoldt, on a : $(\mathcal{X}_\infty)_{\Gamma_n} \simeq T_n$ et $r_n = \dim T_n/pT_n$. Il en résulte en particulier que la suite r_n est croissante. Comme $\mu = 0$, on a un isomorphisme de groupes : $\mathcal{X}_\infty \simeq \mathbb{Z}_p^\lambda$, d’où évidemment $\lim_{n \rightarrow \infty} r_n = \lambda$. \diamond

Nous pouvons maintenant caractériser le “genre un” :

Théorème IV.2 :

Avec les hypothèses précédentes, les propriétés suivantes sont équivalentes :

- a) $\lambda = 1$.
- b) $G_{S_p}(K)$ est un groupe de Demuškin.

Si $\lambda = 1$, le groupe $G_{S_p}(K)$ peut être engendré par deux générateurs y, x liés par une relation $w = x^{\alpha_0}[y, x]$, où le coefficient $\alpha_0 \in \mathbb{Z}_p$ est comme dans 3.4.

Preuve :

a) \Rightarrow b) : si $\lambda = 1$, il résulte du lemme 4.1 que $r = 1$, donc on se retrouve dans la situation de 3.4. Comme $\lambda = 1$, la série caractéristique $f(T)$ de \mathcal{X}_∞ est associée à un polynôme $\alpha_0 + T$ (lemme de Weierstrass). On peut donc choisir des générateurs x, y de G_{S_p} tels que la relation w vérifie $w \equiv x^{\alpha_0}[y, x] \pmod{H_{S_p}^{(2)}}$. Or la nullité de μ signifie que le pro- p -groupe H_{S_p} est libre, de rang égal à λ ; donc $H_{S_p} \simeq \mathbf{Z}_p$, et la congruence précédente est une égalité. En particulier, G_{S_p} est un groupe de Demuškin.

b) \Rightarrow a) : si $G_{S_p}(K)$ est un groupe de Demuškin, tous les groupes $G_{S_p}(K_n)$ sont également de Demuškin. En particulier, $r_n = 1$ pour tout n , donc $\lambda = 1$ d'après 4.1. \diamond

Exemples :

i) **Corps quadratiques réels** ($p = 3$) : voir tableau I.

ii) **Corps cyclotomiques :**

Soit $K = \mathbb{Q}(\mu_p)^+$ et supposons, comme dans l'exemple ii) de 3.4, que la partie moins du p -groupe des classes de $\mathbb{Q}(\mu_p)$ soit cyclique. On voit facilement que cette condition se propage dans la tour cyclotomique, d'où $r_n = 1$ pour tout n , et $\lambda = 1$ d'après 4.1 b).

V.— Genre deux :

K désigne toujours un corps totalement réel vérifiant les hypothèses i) et ii) du §4. On suppose que $\lambda = 2$ et l'on examinera successivement les cas $r = 1, 2$. Outre la série caractéristique $f(T) \in \mathbf{Z}_p[[T]]$ de \mathcal{X}_∞ , il sera commode de faire intervenir des séries à deux variables de $\mathbf{Z}_p[[U, V]]$:

Lemme V.1 : *Supposons $\mu = 0, \lambda = 2$. Alors H_{S_p} est un pro- p -groupe libre de rang 2, engendré par z_1, z_2 , et $H_{S_p}^{(2)}/H_{S_p}''$ (où H_{S_p}'' désigne le second groupe dérivé) est naturellement un $\mathbf{Z}_p[[U, V]]$ -module libre de rang 1, engendré par l'image du commutateur $[z_1, z_2]$.*

Preuve : D'une façon générale, si F est un pro- p -groupe libre de rang $m \geq 2$, engendré par z_1, z_2, \dots, z_m , le quotient $F^{(2)}/F''$, considéré comme module sur l'algèbre complète $\mathbf{Z}_p[[F/F^{(2)}]]$ ($\simeq \mathbf{Z}_p[[U_1, U_2, \dots, U_m]]$), est de dimension projective égale à $m - 2$, donc est libre si et seulement si $m = 2$ ([13], 3.4). Si $m = 2$, un calcul direct montre aussi que l'image de $[z_1, z_2] \pmod{F''}$ forme une base ([5], II thm. 2). \diamond

Proposition V.2 : *Supposons que $\lambda = 2$ et $r = 1$. Alors $G_{S_p}(K)$ peut être engendré par deux générateurs x, y liés par une relation w telle que :*

$$w \equiv x^{\alpha_0} \cdot [y, x]^{\alpha_1} \cdot [y, [y, x]]^{\alpha_2} \cdot [x, [y, x]]^{\beta_0} \pmod{G_{S_p}^{(4)}},$$

où la série caractéristique f de \mathcal{X}_∞ est associée au polynôme distingué $\alpha_0 + \alpha_1 T + \alpha_2 T^2 \in \mathbf{Z}_p[[T]]$, et β_0 est le terme constant d'une certaine série à deux variables $g \in \mathbf{Z}_p[[U, V]]$.

Preuve : On est dans la situation de 3.4. On peut choisir les générateurs x, y de G_{S_p} comme dans 3.4, et l'on peut prendre $z_1 = x, z_2 = [y, x]$ comme générateurs de H_{S_p} . Alors $[z_1, z_2] \in G_{S_p}^{(3)}$. Le même raisonnement que dans 3.4 montre que $w = x^{\alpha_0} \cdot [y, x]^{\alpha_1} \cdot [y, [y, x]]^{\alpha_2} \cdot w'$, avec $w' \in H_{S_p}^{(2)}$. D'après 5.1, il existe une série $g \in \mathbf{Z}_p[[U, V]]$ (où $U = z_1 - 1, V = z_2 - 1$) telle que $w' \equiv g \cdot [z_1, z_2] \pmod{H_{S_p}''}$. Comme $U \cdot [z_1, z_2] = [x, [x, [y, x]]] \in G_{S_p}^{(4)}$ et $H_{S_p}'' \subset G_{S_p}^{(6)}$, la proposition est démontrée. \diamond

Proposition V.3 : *Supposons que $\lambda = r = 2$. Alors $G_{S_p}(K)$ peut être engendré par trois générateurs y, x_1, x_2 liés par deux relations indépendantes w_1, w_2 qui vérifient les propriétés suivantes :*

- il existe deux séries $g_j \in \mathbf{Z}_p[[U, V]]$, $j = 1, 2$,

- il existe une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans \mathbf{Z}_p telle qu'en posant

$x'_1 = x_1^a x_2^b, x'_2 = x_1^c x_2^d$, on ait, pour $j = 1, 2$:

$$w_j \equiv x_j^{\alpha_j} [y, x'_j] \cdot [x_1, x_2]^{\beta_0^j} \cdot [x_1, [x_1, x_2]]^{\beta_1^j} \cdot [x_2, [x_1, x_2]]^{\beta_2^j} \pmod{G_{S_p}^{(4)}},$$

où le polynôme distingué $(\alpha_1 + T)(\alpha_2 + T) \in \mathbf{Z}_p[T]$ est associé à la série caractéristique $f(T)$ de \mathcal{X}_∞ , et $g_j(U, V) = \beta_0^j + \beta_1^j U + \beta_2^j V + \dots$

Preuve : On se trouve ici dans la situation de 3.3. On choisit des générateurs y, x_1, x_2 de G_{S_p} comme dans 3.3. D'après le théorème de structure des \wedge -modules et le lemme de stabilisation 3.1, \mathcal{X}_∞ contient un sous- \wedge -module élémentaire d'indice fini $E = \wedge / (\alpha_1 + T) \oplus \wedge / (\alpha_2 + T)$ de base \bar{x}'_1, \bar{x}'_2 (les α_j sont associés aux diviseurs élémentaires du groupe abélien $T_{S_p}(K)$). Comme \mathcal{X}_∞ et E sont isomorphes à \mathbf{Z}_p^2 en tant que \mathbf{Z}_p -modules, il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans \mathbf{Z}_p telle que $\bar{x}'_1 = \bar{x}_1^a \bar{x}_2^b, \bar{x}'_2 = \bar{x}_1^c \bar{x}_2^d$. La détermination des relations se fait comme dans 5.2. Il reste à montrer que les relations ainsi obtenues sont indépendantes. Or la matrice des relations \mathcal{R} (dans la base \bar{x}_1, \bar{x}_2) est le produit de A par la matrice $\begin{pmatrix} \alpha_1 + T & 0 \\ 0 & \alpha_2 + T \end{pmatrix}$, donc $\det \mathcal{R} \neq 0$ et \mathcal{R} représente un homomorphisme injectif. \diamond

Remarque : D'après le lemme 4.1 b), la situation de la proposition 5.3 se produit toujours, quitte à remplacer K par une extension $K_n, n \gg 0$. Autrement dit, dans tous les cas, 5.3 décrit un sous-groupe d'indice fini de $G_{S_p}(K)$.

Problème : Donner une interprétation arithmétique des coefficients β_j (ou mieux, des séries à deux variables G_j) intervenant dans 5.2 et 5.3. Y a-t-il des liens avec la théorie d'Ihara ?

VI.— Corps IEL, ISS et IWL :

Un des inconvénients de l'énoncé 5.3 réside dans la matrice A . Cette complication technique disparaît si A est diagonalisable. Il est donc naturel de poser les définitions suivantes :

DÉFINITION VI.1 : *Le corps K vérifie toujours les hypothèses du §4. Il sera appelé :*

a) **IEL (Iwasawa élémentaire)** si le \wedge -module \mathcal{X}_∞ est élémentaire, i.e. est isomorphe à un module de la forme $\bigoplus_{i=1}^h \wedge / (f_i(T))$, où les $f_i(T) \in \mathbf{Z}_p[T]$ sont des polynômes distingués irréductibles.

b) **ISS (Iwasawa semi-simple)** si \mathcal{X}_∞ est élémentaire et si les $f_i(T)$ sont linéaires.

Exemples :

- i) Si $r = 1$, K est IEL. Dans ce cas, il sera ISS si et seulement si $\lambda = 1$ (voir 4.2 et 5.2).
- ii) Supposons que K/\mathbb{Q} est abélienne, de groupe de Galois G , et que p ne divise pas l'ordre de G . Il est clair que $T_{S_p}(K)$ est $\mathbf{Z}_p[G]$ -monogène si et seulement si \mathcal{X}_∞ est $\wedge[G]$ -monogène. Si tel est le cas, on dira que K est IWL (ou vérifie la **condition d'Iwasawa-Leopoldt** ; voir b) ci-dessous). Si K est IWL, alors K est visiblement IEL.

Des exemples de corps IWL ont été étudiés par Coates et Lichtenbaum [2] dans le cadre de la “conjecture principale” :

a) Corps quadratiques réels :

Soit $p = 3$, et soit K un corps quadratique réel dont le discriminant D vérifie : $D \not\equiv 0 \pmod{3}$ ou $D = 3(3m + 1)$ ($m \in \mathbf{N}$). En notant $C\ell(\cdot)$ le p -groupe des classes, on a : $C\ell^-(K(\mu_3)) \simeq C\ell(\mathbb{Q}(\sqrt{-3D}))$, par “Spiegelung” (voir la suite exacte (2) de 2.2), on voit facilement que K est IWL si et seulement si $C\ell(\mathbb{Q}(\sqrt{-3D}))$ est nul ou cyclique (auquel cas $r = 0$ ou 1).

b) Corps cyclotomiques :

Prenons $K = \mathbb{Q}(\mu_p)^+$; posons $L_n = \mathbb{Q}(\mu_{p^{n+1}})$ pour tout $n \geq 0$, et notons A_n le p -groupe des classes de L_n . Une **hypothèse standard** (dite d'**Iwasawa-Leopoldt**) dit que, pour tout caractère impair χ de $\Delta = \text{Gal}(L_0/\mathbb{Q})$, la χ -composante $A_0(\chi)$ (donc aussi toute $A_n(\chi)$, par propagation évidente dans la tour cyclotomique) est cyclique. Cette hypothèse est entraînée, par “Spiegelung”, par la **conjecture de Vandiver**, qui dit que $A_n(\varphi) = (0)$ pour tout caractère φ pair. Par “Spiegelung” également, l'hypothèse d'Iwasawa-Leopoldt équivaut à dire que K est IWL.

- c) La situation de b) peut se généraliser : supposons que K/\mathbb{Q} est abélienne, de groupe de Galois G , $p \nmid \#G$ et $K = K(\mu_p)^+$. Supposons que les places de K au-dessus de p sont non-décomposées dans $K(\mu_p)$, totalement ramifiées dans K_∞ , et que la partie moins du p -groupe des classes de $K(\mu_p)$ est

$\mathbf{Z}_p[G]$ -monogène. Alors K est IWL. En effet, avec nos hypothèses (qui se propagent dans la tour cyclotomique), nous savons que le Λ -module $X_\infty^- = \varprojlim A_n^-$ (mêmes notations que dans b)) est G -monogène, et que \mathcal{X}_∞ et X_∞^- sont adjoints (voir la suite exacte (2) de 2.2, ou [15], 4.4).

- iii) Prenons $K = \mathbb{Q}(\mu_p)^+$, $p < 125000$. Alors non seulement K vérifie la conjecture de Vandiver (donc est IWL, donc IEL), mais K est également ISS (voir [22], coroll. 10-17, p. 201). D'une certaine façon, on peut dire que ce phénomène est la règle générale dans la situation IWL, quitte à étendre le corps de base. En effet :

Proposition VI.2 : *Supposons que K est IWL. Alors K_n est ISS pour tout $n \gg 0$.*

Preuve : On a vu que si K est IWL, tous les K_n sont IEL. Prenons $n \gg 0$ pour que $r_n = \lambda$ (notations du lemme 4.1). On a : $\mathcal{X}_\infty \simeq \bigoplus_{i=1}^{r_n} \Lambda_n / (f_i(T))$, où $\Lambda_n = \mathbf{Z}_p[[\Gamma_n]]$. Comme $r_n = \lambda$, chaque f_i est nécessairement de degré 1. \diamond

L'intérêt de la notion ISS provient de la description suivante :

Proposition VI.3 : *Supposons que K est ISS. Alors nous pouvons choisir des générateurs y, x_1, \dots, x_r de $G_{S_p}(K)$ de façon que $G_{S_p} / H_{S_p}^{(2)} \simeq \underset{\langle y \rangle}{*}_{1 \leq j \leq r} \mathcal{D}(\alpha_j; x_j, y)$, où :*

- le polynôme distingué $\prod_{j=1}^r (\alpha_j + T) \in \mathbf{Z}_p[T]$ est associé à la série caractéristique de \mathcal{X}_∞ ,
- le groupe $\mathcal{D}(\alpha; x, y)$ est le groupe de Demuškin engendré par x et y , avec la relation $w = x^\alpha[y, x]$,
- la notation $\underset{H}{*}$ désigne la somme amalgamée par rapport au sous-groupe H (nous sommes dans une situation où la somme amalgamée existe ; voir [18]).

Preuve : On est dans la situation de 3.3 : G_{S_p} est engendré par les d générateurs y, x_1, \dots, x_r liés par r relations indépendantes w_j telles que $w_j \equiv x^{\alpha_j}[y, x_j] \pmod{(G_{S_p}^{(m)} \cdot H_S^{(2)})}$ pour tout m : c'est bien la description annoncée de $G_{S_p} / H_{S_p}^{(2)}$. \diamond

Exemple : Prenons $K = \mathbb{Q}(\mu_p)^+$, $p < 125000$. Alors K est ISS, et de plus $r = \lambda = i(p)$ (l'indice d'irrégularité de p) ([22], p. 201). Soient j_1, \dots, j_λ les entiers pairs $2 \leq j \leq p-3$ tels que p divise le nombre de Bernoulli B_j . Alors, pour $j = j_1, \dots, j_\lambda$, on a : $\alpha_j \sim L_p(1, \omega^{1-j})$, où ω est le caractère de Teichmüller.

Tableau I :

Dans ce tableau on donne, pour $p = 3$ et pour certains corps quadratiques réels $K = \mathbb{Q}(\sqrt{d})$, les valeurs de $r = r(G_{S_p}(K))$ et de $\lambda = \lambda(\mathcal{X}_\infty)$. Les exemples sont extraits de [4] (directement) et [7] (après "Spiegelung").

d	r	λ
2	1	1
29	1	1
62	1	2
82	1	1
103	1	2
122	1	1
257	1	1
717	2	6

Bibliographie

- [1] **J. Coates** : *p-adic L-functions and Iwasawa's theory*, in "Algebraic Number Fields", A. Fröhlich ed., Academic Press (1977), 269-353.
- [2] **J. Coates & S. Lichtenbaum** : *On ℓ -adic zeta functions*, Ann. Math. 98 (1973), 498-550.
- [3] **A. Fröhlich** : *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Math. 24, AMS (1983).
- [4] **D. Hémard** : *Modules galoisiens de torsion et plongements dans les \mathbb{Z}_p -extensions*, J. Number Theory, 30, 3 (1988), 357-374.
- [5] **Y. Ihara** : *Profinite braid groups, Galois representations and complex multiplication*, Ann. Math., 123 (1986), 43-106.
- [6] **K. Iwasawa** : *On \mathbb{Z}_ℓ -extensions of algebraic number fields*, Ann. Math., 98 (1973), 246-326.
- [7] **S. Kobayashi** : *Calcul approché de la série d'Iwasawa pour les corps quadratiques ($p = 3$)*, Sémin. Théorie des Nombres Besançon (1981-82), 64 p..
- [8] **H. Koch** : *Galoissche Theorie der p -Erweiterungen*, VEB Deutscher Verlag der Wissen., Berlin, 1970.
- [9] **K. Komatsu** : *On the maximal p -extensions of real quadratic fields unramified outside p* , J. Algebra, 123 (1989), 240-247.
- [10] **L.V. Kuz'min** : *Local extensions associated with ℓ -extensions with given ramification*, Math. USSR Izv., 9, 4 (1975), 693-726.
- [11] **B. Mazur & A. Wiles** : *Class-fields of abelian extension of \mathbb{Q}* , Invent. Math., 76 (1984), 179-330.
- [12] **A. Movahhedi & T. Nguyen Quang Do** : *Sur l'arithmétique des corps de nombres p -rationnels*, dans "Séminaire de Théorie des Nombres de Paris" 1987-88, C. Goldstein ed., Birkhäuser (1990), 155-200.
- [13] **T. Nguyen Quang Do** : *Formations de classes et modules d'Iwasawa*, dans "Number Theory, Noordwijkerhout 1983", Springer LNM n° 1068 (1984), 167-185.
- [14] **T. Nguyen Quang Do** : *Sur la \mathbb{Z}_p -torsion de certains modules galoisiens*, Ann. Inst. Fourier, 36, 2 (1986), 27-46.
- [15] **T. Nguyen Quang Do** : *Sur la torsion de certains modules galoisiens II*, dans "Séminaire de Théorie des Nombres de Paris" 1986-87, C. Goldstein ed., Birkhäuser (1989), 271-297.
- [16] **T. Nguyen Quang Do** : *Sur la cohomologie de certains modules galoisiens p -ramifiés*, dans "Théorie des Nombres", Laval (1987), J. M. de Koninck & C. Levesque ed., W. de Gruyter (1989), 740-754.

- [17] **T. Nguyen Quang Do** : *Lois de réciprocité primitives* , à paraître dans *Manuscripta Math.* (1991).
- [18] **L. Ribes** : *Amalgamated products of profinite groups* , *Math. Zeit.*, 123 (1971), 357-364.
- [19] **J.-P. Serre** : “*Cohomologie Galoisienne*” , Springer LNM n° 5 (1964).
- [20] **V.-M. Tsvetkov** : *Examples of extensions with Demuškin groups* , *J. Soviet Math.*, 24, 4 (1984), 480-482.
- [21] **S.-V. Ullom & S.-B. Watt** : *Generators and relations for certain class two Galois groups* , *J. London Math. Soc.* 34 (1986), 235-244.
- [22] **L. Washington** : “*Introduction to cyclotomic fields*” , Springer GTM n° 83 (1982).
- [23] **A. Wiles** : *The Iwasawa conjecture for totally real fields* , *Ann. Math.*, 131 (1990), 493-540.
- [24] **K. Wingberg** : *On Galois groups of p -closed algebraic number fields with restricted ramification* , *J. reine angew. Math.*, 400 (1989), 195-202.

Université de Franche-Comté
URA 741 CNRS
Laboratoire de Mathématiques
F - 25030 BESANCON Cédex