SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

ROLAND GILLARD

Problème de plongement et contraintes galoisiennes sur le groupe des classes

Séminaire de théorie des nombres de Grenoble, tome 2 (1972-1973), exp. n° 1, p. 1-6

<http://www.numdam.org/item?id=STNG_1972-1973__2__A1_0>

Roland GILLARD

8 mars 1973

PROBLEME DE PLONGEMENT ET CONTRAINTES GALOISIENNES SUR LE GROUPE DES CLASSES

I - UN PROBLEME DE PLONGEMENT.

Soit p un nombre premier impair et soit E le groupe d'ordre p^3 engendré par trois éléments a,b,c vérifiant les relations :

$$a^p = b^p = c^p = 1 \ , \quad aba^{-1}b^{-1} = c \ , \quad ac = ca \ , \quad bc = cb \ .$$

Soit A le sous-groupe engendré par c, c'est le centre de E. Soit $G = E/A$, G est un groupe de type (p,p). Soit $K/\mathbb{Q}$ une extension galoisienne de type (p,p).

Théorème 1.

Le corps K se plonge dans une surextension galoisienne sur $\mathbb{Q}$ de groupe de Galois isomorphe à E si et seulement si toutes les places de $\mathbb{Q}$ premières à p sont décomposées (partiellement ou totalement) dans K.

Démonstration : On renvoie à [2] pour la méthode et les notations.

Le sous-groupe A étant le centre de E, G agit trivialement sur A. L'action sur les caractères de A se fait donc par action galoisienne sur les racines de l'unité on a donc $L = \mathbb{Q}(\zeta)$ avec ζ racine $p^{\text{ième}}$ de l'unité. Ainsi, L étant cyclique sur $\mathbb{Q}$, le problème de plongement se ramène à la vérification des conditions locales :

1. Condition locale pour une place totalement décomposée dans $K/\mathbb{Q}$: on sait que pour une telle place la condition locale est toujours vérifiée (cf. [2] chap.I, th.4).

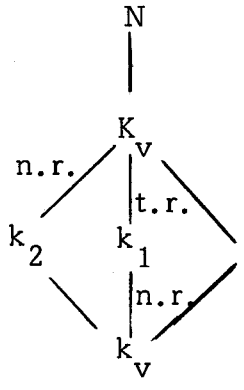
2. Condition locale pour une place partiellement décomposée dans $K/\mathbb{Q}$: soit ϵ l'élément de $H^2(G,A)$ représentant l'extension E de A par G, on sait que pour toute place v la condition locale est équivalente à la condition d'annulation des $\Lambda_{v,\chi}(\epsilon)$ pour tout $\chi \in \hat{A}_v$; l'application $\Lambda_{v,\chi}$ étant donnée par :

$$H^2(G,A) \xrightarrow{\text{res}} H^2(G_v,A) \xrightarrow{\text{inf}} H^2(\Gamma'_v,A) \longrightarrow H^2(\Gamma'_v,K'^*_v) .$$

Or l'image de ϵ par la restriction de G à G_v est nulle. En effet, soit E_v l'image réciproque de G_v dans E, E_v est un sous-groupe de E d'ordre p^2 donc de type (p,p) on a donc $E_v \simeq A \times G_v$. L'élément qui représente E_v comme extension de A par G_v est donc nul dans $H^2(G_v,A)$, or c'est res ϵ. Ainsi res $\epsilon = 0$, de là $\Lambda_{v,\chi}(\epsilon) = 0$. La condition locale est donc vérifiée.

3. Condition locale pour la place associée à p. Comme $\mathbb{Q}_p$ ne contient pas de racine $p^{\text{ième}}$ de l'unité et que G opère trivialement sur A, le seul caractère invariant par Γ'_v est trivial : pour tout χ dans $\hat{A}_v$ on a donc $\Lambda_{v,\chi}(\epsilon) = 0$: la condition locale est vérifiée.

4. Condition locale pour une place première à p et non décomposée dans $K/\mathbb{Q}$. La remarque finale de [2] chap.I montre que la condition locale est vérifiée si et seulement si le problème de plongement relatif à K_v/k_v et E admet une solution. Il est clair que K_v/k_v est ramifiée avec l'indice p. Soit k_1 la sous-extension non ramifiée maximale de K_v et soit k_2 une sous-extension de degré p sur k_v distincte de k_1. Si le problème de plongement local admet une solution N on a le schéma :



Si N/K_v est non ramifiée N/k_2 aussi donc E contient un sous-groupe cyclique d'ordre p^2 : contradiction.

Si N/K_v est totalement ramifiée N/k_1 aussi et on arrive à la même contradiction : en conclusion le problème de plongement local ne peut pas avoir de solution et la condition locale n'est jamais vérifiée.

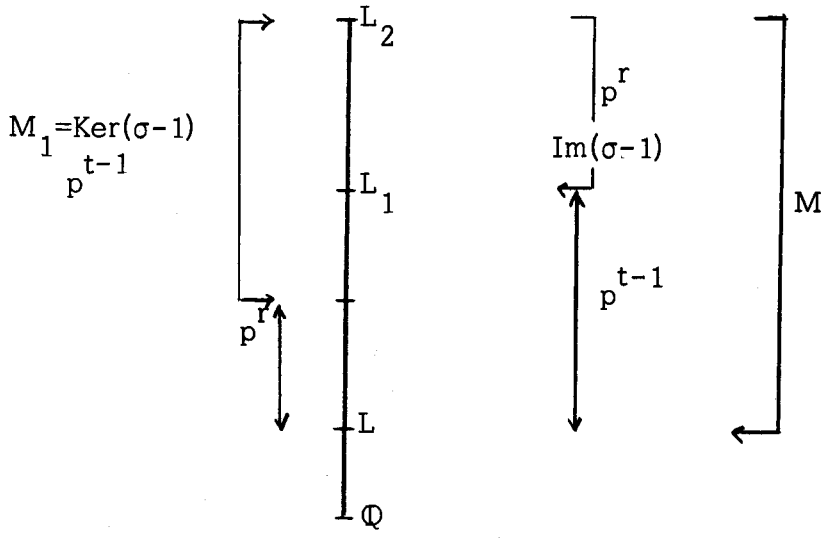
Finalement, pour que les conditions locales soient vérifiées, il faut et il suffit qu'aucune place ne rentre dans le type 4, ci-dessus d'où le théorème 1.

II - CONTRAINTES GALOISIENNES SUR LE GROUPE DES CLASSES.

Soit $L/\mathbb{Q}$ une extension cyclique de degré p premier impair ramifiée seulement en $p_1,\ldots,p_t$. On désigne par σ un générateur du groupe de Galois. Soit $\mathcal{H}$ la composante p-primaire du groupe des classes de L et $\mathcal{H}'$ la somme des autres composantes primaires. L'élément σ opère sur $\mathcal{H}$ et on peut introduire (cf [1]) les sous-groupes : $\mathcal{H}_i = \mathrm{Ker}(\sigma-1)^i$ et $\mathcal{H}_{(i)} = \mathrm{Im}(\sigma-1)^i$ on a la relation sur les indices : $[\mathcal{H}:\mathcal{H}_{(i)}] = [\mathcal{H}_i:1]$.

Dans la suite, on suppose que $\mathcal{H}$ est distinct de $\mathcal{H}_1$ ou ce qui revient au même (cf [1]) que $\mathcal{H}_2$ est distinct de $\mathcal{H}_1$ donc que $\mathcal{H}_{(1)}$ contient strictement $\mathcal{H}_{(2)}$ on note : $p^r = [\mathcal{H}_{(1)}:\mathcal{H}_{(2)}]$. On appelle L_1 et L_2 les extensions abéliennes de L associées par la théorie du corps de classes à $\mathcal{H}_{(1)}\mathcal{H}'$ et $\mathcal{H}_{(2)}\mathcal{H}'$. On pose $M = \mathcal{H}/\mathcal{H}_{(2)}$ et on

observe que $(\sigma-1)^2$ étant nul dans M , on a dans M : $M_1 = \mathrm{Ker}(\sigma-1) \supset \mathrm{Im}(\sigma-1)$. On peut faire le schéma suivant :



Théorème 2.

On a $r \leq t-1$. De plus, le groupe de Galois $G(L_2/\mathbb{Q})$ de $L_2/\mathbb{Q}$ est engendré par $t+r$ éléments $a, b_1 \ldots b_r, c_1 \ldots c_{t-1}$ vérifiant les relations : $a^p = b_1^p = \ldots = b_r^p = c_1^p = \ldots = c_{t-1}^p = 1$.

$$ab_i a^{-1} b_i^{-1} = c_i \quad \text{pour} \quad i = 1 \ldots r$$

$$ac_i = c_i a \quad \text{pour} \quad i = 1 \ldots t-1$$

$$b_i b_j = b_j b_i \quad \text{pour} \quad i,j = 1 \ldots r$$

$$c_i c_j = c_j c_i \quad \text{pour} \quad i,j = 1 \ldots t-1$$

$$b_i c_j = c_j b_i \quad \text{pour} \quad i = 1 \ldots r \ , \ j = 1 \ldots t-1 \ .$$

La suite va montrer comment on peut choisir les éléments $a, b_1 \ldots b_r, c_1 \ldots c_{t-1}$.

Démonstration : L'inégalité $r \leq t-1$ provient de l'inclusion $\mathrm{Ker}(\sigma-1) \supseteq \mathrm{Im}(\sigma-1)$. Observons qu'on peut relever σ en un élément a d'un groupe d'inertie de $L_2/\mathbb{Q}$. On aura alors $a^p = 1$. L'action de σ sur $\mathcal{H}/\mathcal{H}_{(2)} = M$ se lit alors comme la conjugaison par a dans $G(L_2/\mathbb{Q})$.

D'après notre hypothèse on a $M_1 \subsetneq M$ on voit facilement que ceci implique que le centre de $G(L_2/\mathbb{Q})$ est inclus dans M donc est en fait M_1. On sait (cf [1]) que M est un groupe d'exposant p. Comme M/M_1 est d'ordre p^r c'est un espace vectoriel sur Z/pZ de dimension r : on peut trouver des éléments $b_1 \ldots b_r$ de M dont les images dans M/M_1 forment une base. En prenant l'image par $(\sigma-1)$ on obtient une base $c_1 \ldots c_r$ de $\mathrm{Im}(\sigma-1)$: on a $c_i = (\sigma-1)b_i = ab_ia^{-1}b_i^{-1}$ pour $i = 1 \ldots r$. Complétons cette base en une base de M_1 soit $c_1 \ldots c_r c_{r+1} \ldots c_{t-1}$. Il est alors clair que $b_1 \ldots b_r c_1 \ldots c_{t-1}$ forment une base de M. Les éléments $a, b_1 \ldots b_r, c_1 \ldots c_{t-1}$ engendrent donc $G(L_2/\mathbb{Q})$. Les éléments $b_1 \ldots b_r, c_1 \ldots c_{t-1}$ étant dans M commutent entre eux. Les éléments $c_1 \ldots c_{t-1}$ étant dans M_1 commutent avec a. Les éléments b_i, $i = 1 \ldots r$ ne commutent pas avec a : $ab_ia^{-1}b_i^{-1} = c_i$ $(i = 1 \ldots r)$. On a donc obtenu toutes les relations du théorème 2. Puisque $G(L_2/\mathbb{Q})$ est d'ordre p^{r+t} il n'y en a pas d'autre.

On retrouve alors un résultat de [1] :

Théorème 3.

Supposons que $p_1 \ldots p_t$ soient tous distincts de p. Si r est égal à $t-1$, alors pour tout couple (i,j), $i,j = 1, \ldots, t-1$, $i \neq j$, p_i est puissance $p^{\text{ième}}$ modulo p_j et p_j puissance $p^{\text{ième}}$ modulo p_i.

Démonstration : Soient $T_1 \ldots T_t$ les groupes de ramification des nombres premiers $p_1 \ldots p_t$ dans $L_1/\mathbb{Q}$. Soient $\bar{a}, \bar{b}_1, \ldots, \bar{b}_{t-1}$ les images de $a, b_1 \ldots b_{t-1}$ dans le groupe de Galois $G(L_1/\mathbb{Q})$ de $L_1/\mathbb{Q}$. Il est facile de voir qu'on peut choisir $a, b_1 \ldots b_{t-1}$ tels que :

$$\bar{a} \in T_1 \ , \ \bar{a}\bar{b}_1 \in T_2 \ \ldots \ \bar{a}\bar{b}_{t-1} \in T_t \ .$$

Soit K_1 la sous-extension de L_1 ramifiée seulement en p_1. Ainsi dans $L_2/\mathbb{Q}$, L correspond au sous-groupe engendré par $b_1 \ldots b_{t-1}, c_1 \ldots c_{t-1}$ et K_1 au sous-groupe engendré par $ab_1 \ldots ab_{t-1}, c_1 \ldots c_{t-1}$. Soit K le composé $K_1.L$, il correspond au sous-groupe engendré par $b_1^{-1}b_2, \ldots, b_1^{-1}b_{t-1}, c_1 \ldots c_{t-1}$. Soit N la sous-extension de $L_2/\mathbb{Q}$ correspondant au sous-groupe (distingué) engendré par $b_1^{-1}b_2 \ldots b_1^{-1}b_{t-1}$,

$c_1^{-1}c_2\ldots c_1^{-1}c_{t-1}$. Il est clair que N est une extension galoisienne de $\mathbb{Q}$ de groupe de Galois isomorphe à E et que N contient K : d'après I th.1 dans K toute place première à p est décomposée donc en particulier $p_2\ldots p_t$. Comme $L/\mathbb{Q}$ est ramifiée en ces places et non $K_1/\mathbb{Q}$ on voit que $p_2\ldots p_t$ se décomposent dans $K_1/\mathbb{Q}$: ceci implique que $p_2\ldots p_t$ soient des puissances $p^{\text{ièmes}}$ modulo p_1 . En échangeant les rôles de $p_1\ldots p_t$ dans le raisonnement précédent on obtient donc le théorème 3.

En fait [1] énonce la réciproque du théorème 3.

Pour $p = 2$, on peut développer une théorie analogue, on retrouve alors des résultats de [3].

BIBLIOGRAPHIE

[1] - GRAS - "Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ ". Thèse 72 Grenoble.

[2] - GILLARD - "Sur le problème du plongement". Séminaire de théorie des nombres. Grenoble, 72.

[3] - REDEI-REICHARDT - "Die Anzahl..." J. reine angew Math. 170 (1933), 69-74.
