Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Roland Gillard

Sur le problème de plongement

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 2 (1972-1973), exp. n° G11, p. G1-G5

<http://www.numdam.org/item?id=SDPP_1972-1973__14_2_A18_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de Théorie des nombres)
14e année, 1972/73, n° G11, 5 p.

22 janvier 1973

SUR LE PROBLÈME DE PLONGEMENT

par Roland GILLARD

On étudie le plongement d'une extension galoisienne dans une surextension à Groupe de Galois donné.

1. Le problème de plongement.

Soient E un groupe, A un sous-groupe distingué, G le quotient E/A. Soit K/k une extension galoisienne de groupe de Galois isomorphe à G. On dit que le problème de plongement, relatif à K/k et E, admet une solution s'il existe une surextension galoisienne de k, de groupe de Galois isomorphe à E et telle qu'on ait un diagramme commutatif :

$$\begin{array}{l} \text{restriction} \\ \text{des automorphismes} \end{array} \quad \begin{array}{ccc} G(N/k) & \simeq & E \\ \downarrow & & \downarrow \\ G(K/k) & \simeq & G \end{array} \quad \text{passage au quotient .}$$

On supposera dans la suite que E est fini et A commutatif. La conjugaison dans E permet de munir A d'une structure de G-module. L'extension E de A par G est définie à isomorphisme près (cf. ARTIN-TATE [1], chapitre XIII) par un élément ε de $H^2(G, A)$. Soient $\overline{k}$ une clôture algébrique de k, et $\overline{G}$ le groupe de Galois de $\overline{k}/k$. Par l'homomorphisme $\overline{G} \to G$, on peut munir A d'une structure de $\overline{G}$-module. De plus on a une inflation :

$$H^2(G\ ,\ A) \xrightarrow{\inf} H^2(\overline{G}\ ,\ A)$$

THÉORÈME 1 (cf [3]). - *Supposons que K/k soit une extension de corps de nombres, ou que A et G soient des p-groupes (p premier) de même rang. Dans ces conditions, pour que le problème de plongement relatif à K/k et E admette une solution, il faut et il suffit que $\inf \varepsilon$ soit nul.*

2. Localisation.

On suppose que K/k est une extension de corps de nombres. On introduit les notations suivantes : soient n l'exposant de A, ζ une racine primitive n-ième de l'unité, k' et K' les corps $k(\zeta)$ et $K(\zeta)$, et Γ' le groupe de Galois de K'/k.

Pour toute place v de k, on choisit un prolongement, encore noté v, à $\overline{k}$, correspondant à des groupes de décomposition G_v, $\overline{G}_v$, Γ'_v dans G, $\overline{G}$, Γ'. Soit $\hat{A}$ le groupe des caractères $\mathrm{Hom}(A, \overline{k}^*)$; $\overline{G}$ opère sur $\hat{A}$ par

$$\forall\ a \in A,\ \forall\ \chi \in \hat{A},\ \forall\ \sigma \in \Gamma' \qquad (\sigma\chi)(a) = \sigma[\chi(\sigma^{-1} a)] .$$

Cette action passe en fait au quotient : Γ' opère de façon analogue sur $\hat{A}$. Soit $\hat{A}_v$ le sous-groupe de $\hat{A}$ des caractères χ invariants par Γ'_v. Soit L le sous-corps de K' associé au sous-groupe de Γ' laissant fixes tous les éléments de $\hat{A}$. Soient Γ le groupe de Galois de L/k, et Γ_v le complété pour la place v. Considérons alors l'application h, produit des restrictions :

$$h : H^2(\overline{G}, A) \xrightarrow{\prod res} \prod_v H^2(\overline{G}_v, A)$$

On a le résultat suivant.

THÉORÈME 2 (cf [3]). - Si les indices $[\Gamma : \Gamma_v]$ sont premiers entre eux dans leur ensemble (ce qui est vérifié si Γ est cyclique), h est injective. La réciproque est vraie si A est un p-groupe cyclique.

On va utiliser le théorème 2 pour remplacer la condition $\inf \varepsilon = 0$ par la condition $h(\inf \varepsilon) = 0$. Considérons le diagramme :

$$\begin{array}{ccc} H^2(G, A) & \xrightarrow{res} & H^2(G_v, A) \\ \downarrow \inf & & \downarrow \inf \\ H^2(\overline{G}, A) & \xrightarrow{res} & H^2(\overline{G}_v, A) \end{array}$$

Soit ε_v la restriction de ε dans $H^2(G_v, A)$. Appelons condition locale en v, la condition d'annulation de $\inf \varepsilon_v$ dans $H^2(\overline{G}_v, A)$. Pour toute place v, et tout χ dans $\hat{A}_v$, considérons l'application $\Lambda_{v,\chi}$:

$$\Lambda_{v,\chi} : H^2(G, A) \xrightarrow{res} H^2(G_v, A) \xrightarrow{inf} H^2(\Gamma'_v, A) \xrightarrow{H^2(\chi)} H^2(\Gamma'_v, K'^{\hat{*}}_v)$$

On peut énoncer le théorème ci-après.

THEOREME 3. - Si le problème du plongement admet une solution, toutes les conditions locales sont vérifiées. La réciproque est vraie si h est injective. Pour toute place v, la condition locale en v est équivalente à la condition d'annulation des $\Lambda_{v,\chi}(\varepsilon)$ pour chaque χ dans $\hat{A}_v$.

On en déduit le corollaire suivant.

COROLLAIRE. - La condition locale est vérifiée pour toute place v non ramifiée dans K'/k. Il en est de même pour les places totalement décomposées dans K/k.

Démonstration. - Soit v une place non ramifiée dans K'/k : Γ'_v est cyclique. Considérons l'application

$$H^2(\Gamma'_v, A) \xrightarrow{H^2(\chi)} H^2(\Gamma'_v, K'^*_v) \quad \text{pour} \quad \chi \in \hat{A}_v .$$

Pour montrer qu'elle est nulle, on peut utiliser la périodicité de la cohomologie : cette application correspond, sur les $\hat{H}^0$, à :

$$A^{\Gamma'_v}/NA \longrightarrow k_v^*/NK'^*_v .$$

Mais l'image de χ est constituée de racines n-ième de l'unité, donc de normes

(K'/k étant non ramifiée). Cette application est nulle. Il en est donc de même pour $\Lambda_{v,\chi}$.

Soit v une place totalement décomposée dans K/k , G_v est nul : $H^2(G_v , A)$ est nul, donc les applications $\Lambda_{v,\chi}$ sont nulles.

3. Exemples.

(a) Cas où E est extension décomposée de A par G .

THEOREME 4. - Si E est extension décomposée de A par G , le problème de plongement admet une solution.

Démonstration. - Étant donné que ε est nul, inf ε est aussi nul : le théorème 4 résulte alors du théorème 1.

(b) Cas où le plongement est toujours possible.

Soit p un nombre premier. Soit E le groupe à deux générateurs a et b , vérifiant $a^{p^2} = b^p = 1$, $b\, ab^{-1} = a^{1+p}$. Le sous-groupe A , engendré par a^p et b , est distingué. Le quotient G est engendré par l'image de a . L'extension E de A par G est non décomposée. Soit K/k une extension cyclique de degré p de corps de nombres :

THÉORÈME 5. - Le problème de plongement, relatif à K/k et E, admet toujours une solution.

Démonstration. - Le théorème 5 résulte des deux lemmes suivants.

LEMME 1. - Dans les conditions du théorème 5, l'application h est injective.

LEMME 2. - Dans les conditions du théorème 5, les applications $\Lambda_{v,\chi}$ sont nulles.

Démonstration. - On voit immédiatement que Γ' est cyclique, d'où le lemme 1. D'autre part, ceci permet de calculer l'application

$$H^2(\Gamma'_v , A) \xrightarrow{H^2(\chi)} H^2(\Gamma'_v , K'^*_v)$$

pour χ dans $\hat{A}_v$ à l'aide de la cohomologie d'indice 0 :

$$A^{\Gamma'_v} \to k_v^*/NK_v'^* .$$

On peut supposer $G_v \neq \{1\}$. On a alors $G_v = G$, $A^{\Gamma'_v} = A^G$ est donc le sous-groupe engendré par a^p . On vérifie alors que tout caractère χ dans $\hat{A}_v$ (c'est-à-dire invariant par Γ'_v) est trivial sur a^p . Ceci prouve la nullité des $\Lambda_{v,\chi}$ pour tout χ dans $\hat{A}_v$.

(c) Autre exemple.

Désignons par E le groupe engendré par trois éléments a , b , c , vérifiant

les relations (p premier impair) :

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

Soit A le sous-groupe engendré par c (c'est le centre), et désignons par G le quotient : c'est un groupe de type (p , p) . Soit $K/\underset{\sim}{Q}$ une extension du corps des rationnels galoisienne de type (p , p) . On peut alors énoncer le résultat suivant.

THÉORÈME 6. - Pour que le problème de plongement, relatif à $K/\underset{\sim}{Q}$ et E , admette une solution, il faut et il suffit que toute place première à p soit décomposée (partiellement ou totalement) dans $K/\underset{\sim}{Q}$.

Démonstration. - Comme G agit trivialement sur A , on a $L = k(\zeta)$: Γ est cyclique, et l'application est injective. Étudions les conditions locales :

1° G_v d'ordre p : Soit E_v l'image réciproque de G_v dans E , ε_v correspond à l'extension E_v de A par $\mathcal{T}_v$:

$$1 \to A \to E_v \to G_v \to 1 ;$$

E_v est de type (p , p) , cette extension est décomposée : on a $\varepsilon_v = 0$. Les conditions locales sont vérifiées pour les places telles que G_v soit d'ordre 1 ou p .

2° Place au-dessus de p : Comme $\underset{\sim}{Q}_p$ ne contient pas ζ_p , racine p-ième de l'unité, il n'y a pas de caractère invariant autre que le caractère trivial :

$$\chi \in \hat{A}_v \Rightarrow \Lambda_{v,\chi}(\varepsilon) = 0 .$$

La condition locale est vérifiée.

3° G_v d'ordre p^2 , v première à p : Comme toute extension locale non ramifiée, ou totalement et modérément ramifiée, est cyclique, et que G est de type (p , p) , on voit que la place v doit être ramifiée dans K/k avec l'indice p . Soient k_1 la sous-extension non ramifiée de degré p de K/k , et k_2 une sous-extension distincte de k_1 . Comme G_v est égal à G , et que E et G ont même rang, la condition locale est équivalente à l'existence d'une solution N au problème de plongement relatif à $K_v/\underset{\sim}{Q}_v$ et E . Montrons qu'une telle solution N n'existe pas : Si N/K est non ramifiée, N/k_2 est cyclique, et E possède un sous-groupe cyclique d'ordre p^2 : c'est absurde. Si N/K est ramifiée, N/k_1 est totalement et modérément ramifiée, donc cyclique : même contradiction. Ainsi, le problème de plongement local n'admettant pas de solution, la condition locale n'est pas remplie.

Ainsi, pour que le problème de plongement admette une solution, il faut et il suffit que, pour les places premières à p , G_v soit d'ordre 1 ou p : d'où le théorème 6.

BIBLIOGRAPHIE

[1] ARTIN (E.) and TATE (J.). - Class field theory. - New York, Amsterdam, W. A. Benjamin, 1968.

[2] GILLARD (R.). - Sur le problème de plongement, C. R. Acad. Sc. Paris, t. 274, 1972, Série A, p. 1436-1438 (1).

[3] HOECHSMANN (K.). - Zum Einbettungsproblems, J. für reine und angew. Math., t. 229, 1968, p. 81-106.

(Texte reçu le 12 mars 1973)

Roland GILLARD
Institut de Mathématiques pures
Boîte postale 116
38402 SAINT-MARTIN D'HÈRES

---

(1) Cette note est développée dans les Séminaires 1971/72 de l'Institut de mathématiques de Grenoble. La théorie générale des § 1 et 2 y a été plus développée. On y trouve d'autres exemples (extensions abéliennes, extensions quaternioniennes). D'autre part, l'étude complète du cas où E est un groupe d'ordre p^3 (p premier) sera publiée prochainement par l'auteur.