SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

R. GILLARD

Sur le problème de plongement

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 39-60

<http://www.numdam.org/item?id=STNG_1971-1972__1__39_0>

SUR LE PROBLEME DE PLONGEMENT

par Roland GILLARD les 19-26.1.72 et 9.2.72

Le point de départ de cette étude est un article de Hoechsmann [5] qui fait un exposé systématique du problème de plongement en termes de cohomologie.

Dans le premier chapitre, je redonne la définition de ce problème classique et résume l'article de Hoechsmann. Le dernier paragraphe montre comment on peut utiliser pratiquement la théorie générale.

On donne ensuite deux exemples d'application : exemples de plongement dans une extension abélienne ou quaternionique.

I. THEORIE GENERALE.

I.1. Introduction

Rappelons tout d'abord la définition du problème du plongement. On se donne une extension galoisienne K/k de corps commutatifs, de groupe de Galois G. On se donne aussi une suite exacte de groupes :

$$1 \to A \to E \to G \to 1$$

On appelle solution au problème de plongement (P) une surextension galoisienne N de k telle qu'il existe un isomorphisme π, induisant π' sur A rendant le diagramme suivant commutatif :

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E & \to & G & \to & 1 \\ & & \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} & & \downarrow & & \\ 1 & \to & G(N/K) & \to & G(N/k) & \to & G(K/k) & \to & 1 \end{array}$$

On supposera dans toute la suite que E est fini, A étant un sous-groupe abélien.

I.2. Traduction cohomologique

La suite exacte de groupes de I.1. sera décrite (à isomorphisme près) par la structure correspondante de G-module sur A et un élément ε de $H^2(G,A)$, cet élément n'étant nul que si la suite exacte est scindée, E étant alors extension décomposée de A par G.

Soit $\bar{k}$ une clôture algébrique de k, $\bar{G}$ le groupe de Galois de $\bar{k}/k$. Si (P) admet une solution N, on a un diagramme commutatif d'homomorphismes surjectifs des groupes de Galois :

$$\begin{array}{ccc} & \swarrow & \bar{G} \\ & & \downarrow \\ G(N/k) & \to & G \\ \downarrow & & \downarrow \\ E & \to & G \end{array}$$

Il existe donc un homomorphisme surjectif Φ rendant le diagramme suivant commutatif :

$$\begin{array}{ccc} & & \bar{G} \\ & \overset{\Phi}{\swarrow} & \downarrow \\ E & \to & G \end{array} \qquad (D)$$

Réciproquement, si un tel Φ existe en prenant pour N le corps associé à son noyau, on obtient une solution à (P) . A l'aide de [5] 2.3 et 6.7, on peut supprimer l'hypothèse de surjectivité dans les cas suivants :

Lemme 1.

Lorsque K/k est une extension de corps de nombres algébriques ou lorsque G et E sont des p-groupes de même rang, l'existence d'un homomorphisme Φ rendant (D) commutatif entraîne celle d'un homomorphisme surjectif ayant la même propriété.

Considérons le diagramme suivant :

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E \times_G \bar{G} & \xrightarrow{p_2} & \bar{G} & \to & 1 \\ & & \downarrow & & \downarrow{\scriptstyle p_1} & & \downarrow & & \\ 1 & \to & A & \to & E & \to & G & \to & 1 \end{array} \qquad (D_1)$$

Ici $E \times_G \bar{G}$ désigne le sous-ensemble de $E \times \bar{G}$ des couples (e,g) formé d'éléments qui ont même image dans G . Les applications p_1 et p_2 sont les projections. On voit facilement que le diagramme ci-dessus est commutatif et que sa première ligne est aussi exacte. L'opération de $\bar{G}$ sur A correspondante se fait par l'intermédiaire de G . L'élément de $H^2(\bar{G},A)$ qui caractérise cette extension n'est autre que $\inf \epsilon$, image de ϵ par inflation. On peut alors énoncer :

Théorème 1.

Dans les hypothèses du lemme 1, pour que (P) admette une solution, il faut et il suffit que l'image de ϵ par l'inflation suivante soit nulle :

$$H^2(G,A) \to H^2(\bar{G},A) \ .$$

Démonstration :

Si on a un homomorphisme Φ complétant (D) , l'application $\Phi \times Id$ de $\bar{G}$ dans $E \times \bar{G}$ définit une section linéaire pour la suite exacte de la première ligne de (D_1) qui est donc scindée ; l'élément inf ϵ qui la représente dans $H^2(\bar{G},A)$ est donc nul. Réciproquement, si inf ϵ est nul, la suite est scindée, soit s une section linéaire, il est bien clair que $p_1 \circ s$ rend (D) commutatif.

Corollaire 1.

Si E est extension décomposée de A par G , (P) admet toujours une solution dans les hypothèses du lemme 1.

Corollaire 2.

K/k étant ici une extension de corps de nombres si le groupe A se décompose en somme directe de G-modules A_i $(i=1,\ldots,r)$ le problème de plongement relatif à une extension E de A par G est équivalent aux problèmes relatifs à des extensions E_i des A_i par G (ces problèmes devant être tous considérés).

Démonstrations :

Pour le corollaire 1 , il suffit de remarquer que si ϵ est nul, inf ϵ aussi. Pour le corollaire 2 , on observe qu'à la décomposition $A = \overset{r}{\underset{i=1}{\oplus}} A_i$ correspond les décompositions $H^2(G,A) = \overset{r}{\underset{i=1}{\oplus}} H^2(G,A_i)$ et : $H^2(\bar{G},A) = \overset{r}{\underset{i=1}{\oplus}} H^2(\bar{G},A_i)$.

On a donc inf $\epsilon = \oplus$ inf ϵ_i . La nullité de inf ϵ est équivalente à celle des inf ϵ_i . Or si ϵ correspond à l'extension E_i de A_i par G la nullité de inf ϵ_i s'interprète sous forme d'un problème de plongement.

I.3. Localisation du problème

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

sur k . Soit $\hat{A}$ le groupe $\mathrm{Hom}(A,\bar{k}^*)$, les groupes $\bar{G}$ et Γ' opérant sur $\hat{A}$ par $(\sigma\chi)(a) = \sigma\chi(\sigma^{-1}a)$ pour tout χ de $\hat{A}$, tout a de A et tout σ dans Γ' ou $\bar{G}$. Pour chaque place v finie ou non de k , on choisit un prolongement, noté aussi v , à $\bar{k}$, correspondant à des groupes de décomposition G_v , Γ'_v , $\bar{G}_v$ et à des complétés k_v , K_v , K'_v . On désigne aussi par $\bar{k}_v$ une clôture algébrique de K'_v . Soit L le sous-corps de K' associé au sous-groupe de Γ' laissant fixes les éléments de $\hat{A}$. On note par Γ son groupe de Galois sur k , et Γ_v le groupe de décomposition correspondant. Enfin, on désigne par $\hat{A}_v$ le sous-groupe des caractères invariants par Γ'_v .

L'idée de la méthode est d'utiliser l'application h suivante, produit de restrictions dont on peut discuter l'injectivité à l'aide des théorèmes de dualité globale de Poitou et Tate (cf. [6]).

$$H^2(\bar{G},A) \xrightarrow{h} \prod_v H^2(\bar{G}_v,A)$$

Le théorème 6.3 de [5] donne le résultat suivant :

Théorème 2.

Pour que h soit injective, il suffit que les indices $[\Gamma : \Gamma_v]$ soient premiers entre eux dans leur ensemble (ce qui est vérifié notamment dans le cas où Γ est cyclique). La condition est nécessaire si A est un p-groupe cyclique.

I.4. Etude des conditions locales

L'étude de $h(\inf \varepsilon)$, motivée par le théorème 2, peut se faire à l'aide du joli diagramme suivant :

$$\begin{array}{ccccccc}
H^2(G,A) & \to & \prod_v H^2(G_v,A) & \to & \prod_v H^2(\Gamma'_v,A) & \to & \prod_{v,\chi} H^2(\Gamma'_v,K'^*_v) \\
\downarrow & & \searrow & & \swarrow & & \downarrow \\
H^2(\bar{G},A) & \xrightarrow{h} & \prod_v H^2(\bar{G}_v,A) & \longrightarrow & & & \prod_{v,\chi} H^2(\bar{G}_v,\bar{k}^*_v)
\end{array}$$

On passe de la première ligne à la seconde par des inflations. Les premières applications de chaque ligne sont des produits de restrictions. Elles forment avec les inflations un diagramme commutatif résultant des diagrammes :

$$\begin{array}{ccc} \bar{G}_v & \to & \bar{G} \\ \downarrow & & \downarrow \\ G_v & \to & G \end{array}$$

Le triangle central est défini par des produits d'inflations. La commutativité provient de celle du diagramme :

$$\begin{array}{ccc} \bar{G}_v & \to & \Gamma'_v \\ & \searrow & \downarrow \\ & & G_v \end{array}$$

La dernière application de chaque ligne est définie pour le facteur correspondant à v par le produit des caractères dans $\hat{A}_v$. La commutativité résulte ici des propriétés de l'inflation. D'après le théorème de dualité locale de Tate, la dernière application de la seconde ligne est injective (cf. par exemple [6]) ; comme la dernière colonne est injective (cf. [8] X § 5 cor. de prop. 5), la nullité de $h(\inf \varepsilon)$ est équivalente à celle de l'image de ε par l'application de la première ligne. Introduisons donc pour chaque place v et chaque caractère χ dans $\hat{A}_v$ l'application :

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

On peut alors énoncer :

Théorème 3.

Si (P) admet une solution, l'image de ε par $\wedge_{v,\chi}$ est nulle pour toute place v de k et tout caractère χ dans $\hat{A}_v$. La réciproque est vraie si h est injective (cf. par exemple théorème 2).

En fait seul un nombre fini de places fait problème :

Théorème 4.

Si v est non ramifiée dans K'/k, $\wedge_{v,\chi}$ est nulle pour tout χ dans $\hat{A}_v$. Il en est de même si v est totalement décomposée dans K/k.

Démonstration :

Si v est ramifiée dans K'/k, Γ'_v est cyclique. La dernière application entrant dans la définition de $\wedge_{v,\chi}$ peut s'étudier à l'aide de la cohomologie

modifiée d'indice nul :

$$A^{\Gamma'_v}/NA \simeq \hat{H}^0(\Gamma'_v, A) \to \hat{H}^0(\Gamma'_v, K'^*_v) \simeq k^*_v/N_{K'_v/k_v}(K'^*_v) .$$

Cette application est donc induite par χ :

$$A^{\Gamma'_v} \xrightarrow{\chi} k^*_v \to k^*_v/NK'^*_v$$

Or, l'image de χ est constituée de racines de l'unité donc d'unités de k_v donc de normes de K'_v (toujours à cause de l'abscence de ramification). L'application $\wedge_{v,\chi}$ est donc nulle.

Si la place v est totalement décomposée dans K/k , G_v est nul. Donc l'application $\wedge_{v,\chi}$ est nulle.

Remarque :

Soit ϵ_v la restriction de ϵ dans $H^2(G_v, A)$. On sait que ϵ_v correspond à la suite exacte (E_v est l'image réciproque de G_v dans E) :

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

On a donc un problème de plongement local avec K_v/k_v et ϵ_v . On peut remarquer que la condition d'annulation des $\wedge_{v,\chi}(\epsilon)$ provient en fait de l'annulation de $\inf \epsilon_v$ dans $H^2(\bar{G}_v, A)$. Autrement dit, si les conclusions du lemme 1 sont vérifiées pour le problème local de plongement, celui-ci admet une solution si, et seulement si, notre condition locale sur les $\wedge_{v,\chi}$ est vérifiée. Cette remarque sera utile pour simplifier les conditions locales dans le cas où E est une extension abélienne (cf. II).

II. PLONGEMENT DANS UNE SUREXTENSION ABELIENNE.

Dans ce chapitre, on reprend les notations du chapitre I, E étant ici un groupe commutatif, K/k étant une extension de corps de nombres. On dira qu'un groupe est primaire si son ordre est une puissance d'un nombre premier. Comme Richter [7] on réduit le problème au cas où E est cyclique primaire.

II.1. Première réduction

Le groupe A étant abélien, peut se représenter comme somme directe de groupes (donc de G-modules, puisque G agit ici trivialement) cycliques primaires :

$$A = \bigoplus_{i=1}^{I} A_i$$

On utilise alors le corollaire 2 de I. théorème 1, pour se ramener à des problèmes de plongement relatifs à des extensions de A_i par G.

Ceci montre que pour la suite on peut se limiter au cas où A est un groupe cyclique primaire.

II.2. Réduction au cas où E est cyclique primaire

Comme E est abélien on peut le représenter par une somme directe de groupes cycliques primaires :

$$E = \bigoplus_{i=1}^{r} E_i$$

On note a_i un générateur de E_i $(i=1,\dots,r)$. Supposant A cyclique primaire, un de ses générateurs peut s'écrire :

$$a = \sum_{i=1}^{r} x_i a_i \qquad x_i \in \mathbb{N} \quad \text{pour} \quad i=1,\dots,r$$

Soit $n = \ell^\nu$ l'ordre de A, une des composantes au moins de a est d'ordre ℓ^ν soit par exemple $a_1 x_1$. On pose alors :

$$H = A \oplus H' \quad \text{avec} \quad H' = E_2 \oplus \dots \oplus E_r .$$

Soit $\bar{H}$ l'image de H dans G. On note alors :

$$E_1 = E/H' \quad \text{et} \quad G_1 = E/H \simeq G/\bar{H} .$$

On désigne par K_1 le sous-corps de K associé à $\bar{H}$ et par (P_1) le problème de plongement relatif à K_1/k et à E_1 considéré comme extension de A par G_1. On peut alors énoncer la proposition suivante qui établit la possibilité de se ramener au cas où E est cyclique primaire :

Proposition 1.

Pour que le problème (P) admette une solution, il faut et il suffit qu'il en soit de même pour (P_1).

Démonstration :

On a le diagramme commutatif suivant reliant nos deux suites exactes :

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E & \to & G & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & A & \to & E_1 & \to & G_1 & \to & 1 \end{array}$$

Il en résulte que ϵ est l'image par inflation de ϵ_1, représentant de la deuxième ligne dans $H^2(G_1,A)$. Si on considère le diagramme :

$$\begin{array}{ccc} H^2(G_1,A) & \xrightarrow{\text{inf}} & H^2(G,A) \\ & \searrow^{\text{inf}} & \downarrow \text{inf} \\ & & H^2(\bar{G},A) \end{array}$$

On voit que les images de ϵ et ϵ_1 par inflation dans $H^2(\bar{G},A)$ sont nulles en même temps, d'où la proposition d'après le théorème 1 de I.2.

II.3. Etude du cas où E est cyclique primaire

Soient donc $n = \ell^\nu$ et $m = \ell^\mu$ les ordres de A et G. Le groupe E étant abélien, A est un G-module trivial ; $\bar{G}$ opère donc sur $\hat{A}$ par action galoisienne sur les racines de l'unité. On aura donc $L = k(\zeta)$ en reprenant les notations de I.

a) Etude de l'injectivité de h.

Elle se fait à l'aide de I.3., théorème 2 : si ℓ est impair, L est cyclique sur k, et h est injective. Si ℓ est égal à 2 et L cyclique, on conclut de la même façon. Si L n'est pas cyclique, h est injective si, et seulement s'il existe une place v telle que $[\Gamma : \Gamma_v] = 1$. La place v doit donc être non décomposée dans L, ou ce qui revient au même dans la sous-extension bicyclique biquadratique de L. Si v ne divise pas 2, v est non ramifiée dans L donc Γ_v est cyclique donc a priori distinct de Γ. Tout ceci permet d'énoncer :

Proposition 2.

L'application h est injective si, et seulement si, $k(\zeta)$ est cyclique sur k ou, n'étant pas cyclique, possède une place (nécessairement au-dessus de 2) non décomposée dans la sous-extension biquadratique bicyclique de $k(\zeta)/k$.

b) Etude des conditions locales.

Lemme 1.

Si E , extension de A par G , est cyclique primaire, l'élément ϵ associé est un générateur de $H^2(G,A)$.

Démonstration :

Soit ℓ^α le cardinal de $H^2(G,A)$, remarquons que ℓ^α est inférieur ou égal à ℓ^μ , ordre de G . Il s'agit de vérifier que $\ell^{\alpha-1}\epsilon$ $(\alpha>0)$ est non nul. Soit H le sous-groupe de G d'indice $\ell^{\alpha-1}$, $\ell^{\alpha-1}\epsilon$ n'est autre que l'image de ϵ par l'application :

$$H^2(G,A) \xrightarrow{\text{res}} H^2(H,A) \xrightarrow{\text{cor}} H^2(G,A) \ .$$

Mais res ϵ représente en fait l'extension définie par la suite exacte suivante (E' image réciproque de H dans E) :

$$I \to A \to E' \to H \to 1 \quad .$$

Or, E' étant cyclique cette extension n'est pas décomposée : res $\epsilon \neq 0$. Vérifions maintenant que la corestriction est injective :

$$\begin{array}{ccc} H^2(H,A) & \xrightarrow{\text{cor}} & H^2(G,A) \\ \downarrow \wr & & \downarrow \wr \\ A^H/[H].A & \xrightarrow{\text{cor}} & A^G/[G].A \end{array}$$

On a noté [H] et [G] les ordres des groupes H et G . La corestriction s'interprètre en cohomologie modifiée d'ordre 0 comme la norme de G/H , donc ici par la multiplication par $\ell^{\alpha-1}$:

$$A/\ell^{\mu-\alpha+1} \to A/\ell^\mu \ .$$

La corestriction est donc injective : $\mathrm{cor} \circ \mathrm{res}\ \epsilon \neq 0$.

L'intérêt du lemme 1 est de se ramener à l'étude de la nullité des applications $\wedge_{v,\chi}$, sans référence à ϵ :

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

Les seuls caractères à considérer sont ceux de $\hat{A}_v$, invariants par Γ'_v . Or, dire que χ est invariant par Γ'_v revient à dire que son image $\chi(A)$ est dans k_v . On peut donc calculer $\wedge_{v,\chi}$ à l'aide du diagramme commutatif dont la dernière colonne est une inflation injective :

$$\begin{array}{ccccc} H^2(G,A) & \xrightarrow{\text{res}} & H^2(G_v,A) & \xrightarrow{H^2(\chi)} & H^2(G_v,K_v^*) \\ & & \downarrow \text{inf} & & \downarrow \text{inf} \\ & & H^2(\Gamma'_v,A) & \xrightarrow{H^2(\chi)} & H^2(\Gamma'_v,K'^*_v) \end{array}$$

Comme $\mathrm{res}\ \epsilon$ d'après le lemme 1 engendre $H^2(G_v,A)$ la nullité de $\wedge_{v,\chi}(\epsilon)$ est équivalente à celle de l'application $H^2(\chi)$:

$$H^2(G_v,A) \rightarrow H^2(G_v,K_v^*) .$$

Cette application peut s'étudier (G_v étant cyclique) à l'aide de l'application :

$$A/[G_v].A \simeq \hat{H}^0(G_v,A) \xrightarrow{\chi} \hat{H}^0(G_v,K_v^*) \simeq k_v^*/N K_v^*$$

$\wedge_{v,\chi}$ est nulle si, et seulement si, $\chi(A)$ est inclus dans $N K_v^*$ groupe des normes de K_v^* dans k_v^* , ceci devant être vrai pour tout caractère χ invariant par Γ'_v .

Proposition 3.

$\wedge_{v,\chi}(\epsilon)$ est nul pour tout χ de $\hat{A}_v$ si, et seulement si, toutes les racines n$^{\text{ièmes}}$ de l'unité qui sont dans k_v^* sont des normes de K_v^* .

Démonstration :

Elle résulte du fait que toutes les racines n$^{\text{ièmes}}$ de l'unité qui sont dans k_v correspondent à des caractères invariants et réciproquement.

On peut donc énoncer le théorème suivant (cf. [7] et aussi [1] chap. X) :

Théorème 1.

E étant supposé cyclique primaire, si (P) admet une solution alors pour chaque place v de k, les racines $n^{\text{ièmes}}$ de l'unité qui sont dans k_v sont des normes de K_v. Cette condition est suffisante si $k(\zeta)/k$ est cyclique, ou sinon, quand sa sous-extension biquadratique bicyclique possède une place au moins (divisant forcément 2) non décomposée sur k.

c) Autre énoncé des conditions locales pour les places modérément ramifiées.

Soit v une place finie ramifiée modérément avec l'indice e ($e>1$). On va exprimer autrement la condition locale : G_v et E_v étant de même rang (cf. pour les notations fin de I.4.) la condition locale se réduit en fait à un problème de plongement local : une solution de ce problème est une extension cyclique de k_v. On voit alors que nécessairement son indice de ramification est (e.n). L'existence d'une telle solution implique donc que k_v contienne les racines de l'unité d'ordre (e.n) (cf. [2], chap. VI, 2.5. corollaire, chap. I 8. prop. 2 et chap. II appendice C lemme).

Réciproquement, si k_v contient les racines de l'unité d'ordre (e.n), ce sont des normes de la sous-extension non ramifiée maximale de K_v et les racines $n^{\text{ièmes}}$ sont des normes de K_v : la condition locale du b) est remplie ; ainsi on a une condition équivalente :

Proposition 4.

Si v est une place de k, ramifiée modérément avec l'indice e ($e>1$) dans K, pour que les applications $\wedge_{v,\chi}$ pour χ dans $\hat{A}_v$ soient nulles, il faut et il suffit que k_v contienne les racines de l'unité d'ordre (e.n).

Donnons une conséquence de cette proposition : lorsque k est le corps des rationnels en utilisant la proposition 3 pour les places infinies et celle au-dessus de ℓ et la proposition 4 dans les autres cas, on obtient immédiatement le théorème suivant (cf. [7]) :

Théorème 2.

Pour qu'une extension cyclique de degré ℓ^{μ} de $\mathbb{Q}$ se plonge dans une extension cyclique de degré $\ell^{\mu+\nu}$ il faut qu'elle soit totalement réelle et que tout nombre premier q différent de ℓ, ramifié avec l'indice e $(e>1)$ vérifie la congruence :

$$q \equiv 1 \mod(e\ell^{\nu})$$

La condition de réciproque est la même que pour le théorème 1.

III. PLONGEMENT D'UNE EXTENSION QUADRATIQUE DANS UNE EXTENSION QUATERNIONIQUE.

III.1. Introduction

Dans ce chapitre, on appelle groupe quaternionique généralisé, le groupe E_n d'ordre $2n$ (n étant un nombre pair strictement positif) engendré par deux éléments σ et τ vérifiant les relations :

$$\sigma^n = 1$$
$$\tau^2 = \sigma^{n/2}$$
$$\tau\sigma\tau^{-1} = \sigma^{-1}$$

Soit A_n le sous-groupe engendré par σ et $G = \{1, \bar{\tau}\}$, le quotient. G opère donc par symétrie sur A_n. L'extension de A_n par G est non décomposée, l'élément ϵ_n associé dans $H^2(G,A_n)$ n'est donc pas nul. Calculons $H^2(G,A_n)$:

$$H^2(G,A_n) \simeq \hat{H}^0(G,A_n) \simeq A_n^G/NA_n \simeq \{1, \sigma^{n/2}\}$$

On considère une extension quadratique de corps de nombres K/k, et en identifiant son groupe de Galois à G on note (P_n) le problème de plongement relatif à E_n. Le théorème suivant permet de comparer les problèmes relatifs à deux indices :

Théorème 1.

Si (P_n) admet une solution, il en est de même de $(P_{n'})$ pour tout n' multiple de n. La réciproque est vraie si n'/n est impair lorsque n est une puissance de 2 .

Démonstration :

En envoyant un générateur de A_n sur une puissance (n'/n) d'un générateur de $A_{n'}$, on obtient un G-homomorphisme injectif $A_n \to A_{n'}$ qui induit un isomorphisme sur les groupes $\hat{H}^\circ$ donc aussi sur les H^2.

Considérons alors le diagramme commutatif :

$$\begin{array}{ccc} H^2(G,A_n) & \to & H^2(G,A_{n'}) \\ \downarrow \text{inf} & & \downarrow \text{inf} \\ H^2(\bar{G},A_n) & \to & H^2(\bar{G},A_{n'}) \end{array}$$

Il est clair que l'image de ε_n par la première ligne est $\varepsilon_{n'}$. La nullité de $\inf \varepsilon_n$ entraîne donc celle de $\inf \varepsilon_{n'}$, ce qui se traduit (I. th. 1) en disant que si (P_n) admet une solution, $(P_{n'})$ aussi.

Si n'/n est impair, A_n est facteur direct de $A_{n'}$: il existe un sous G-module M de $A_{n'}$ tel que :

$$A_{n'} = M \oplus A_n .$$

On a alors une décomposition des groupes de cohomologie :

$$H^2(G,A_{n'}) = H^2(G,M) \oplus H^2(G,A_n)$$
$$H^2(\bar{G},A_{n'}) = H^2(\bar{G},M) \oplus H^2(\bar{G},A_n) .$$

Dans la première décomposition, d'après la nullité du groupe $H^2(G,M)$ (G étant d'ordre 2 et M d'ordre impair) on a : $\varepsilon_{n'} = 0 \oplus \varepsilon_n$. Ce qui donne : $\inf \varepsilon_{n'} = 0 \oplus \inf \varepsilon_n$. Ainsi $\inf \varepsilon_n$ et $\inf \varepsilon_{n'}$ sont nuls en même temps, d'où la deuxième partie du théorème.

On sait que l'on peut se limiter aux valeurs paires de n. Les paragraphes suivants vont être consacrés à la démonstration du théorème 2 :

Théorème 2.

Pour que (P_n) admette une solution, il faut que toute place réelle de k se prolonge dans $K = k(\sqrt{\alpha})$ en des places réelles. Cette condition étant supposée réalisée, (P_2) admet une solution si, et seulement si, (-1) est une norme de K/k, (P_4) admet une solution si, et seulement si, toute place v de k au-dessus de 2 telle que α soit dans $-(k_v)^2$ a un degré local pair sur le corps des rationnels. Pour que (P_8) admette une solution (c'est le cas si $\alpha = -1$) il suffit qu'il existe une place v (divisant forcément 2α) telle que aucun des nombres 2, $-\alpha$, -2α ne soit dans $(k_v)^2$.

III.2. Etude de la condition sur les places infinies

Soit v une place infinie de k, il s'agit de dire quand la condition locale nécessaire, relative à v est remplie. Si G_v est trivial le théorème 4 de I permet de conclure. Si G_v n'est pas trivial, on a à étudier (cf. I.4. remarque) la nullité de $\inf \varepsilon_v$ dans $H^2(\bar{G}_v, A)$. Or, on a la suite d'applications :

$$H^2(G, A) \xrightarrow[\sim]{\text{res}} H^2(G_v, A) \xrightarrow[\sim]{\inf} (\bar{G}_v, A) .$$

Ces applications sont des isomorphismes, les groupes G_v et $\bar{G}_v$ étant en fait égaux à G. Ainsi $\inf \varepsilon_v$ est l'image de ε par un isomorphisme donc n'est pas nul : pour que la condition locale en v soit remplie, il faut et il suffit que G_v soit trivial.

En considérant toutes les places infinies de k, on obtient donc la condition nécessaire suivante, qui est celle du théorème :

"Pour que (P_n) admette une solution, il faut que toute place réelle de k se prolonge en des places réelles de K ".

III.3. Places modérément ramifiées dans K/k

Soit v une place ramifiée dans K/k ne divisant pas 2. Une telle place est non ramifiée dans $k(\zeta)/k$. Les extensions $k_v(\zeta)$ et K_v sont donc linéairement disjointes sur k_v. Dans Γ'_v, il existe donc un élément $\tilde{\tau}$

opérant non trivialement sur k_v et trivialement sur les racines $n^{\text{ièmes}}$ de l'unité. Un caractère invariant par Γ'_v doit être invariant par $\tilde{\tau}$. On a donc pour tout a de A_n :

$$\chi(a) = (\tilde{\tau}\chi)(a) = \chi^{-1}(a) \qquad \text{i.e.} \quad \chi(a) = \pm 1$$

$\wedge_{v,\chi}$ se factorise donc par l'application :

$$H^2(G_v, A) \xrightarrow{\chi} H^2(G_v, K_v^*) \quad .$$

Cette application s'étudie à l'aide des $\hat{H}^\circ$:

$$\{1, \sigma^{\frac{n}{2}}\} = A^{G_v} \to k_v^* / N K_v^* \quad .$$

Mais, on a $\chi(\sigma) = \pm 1$ d'où $\chi(\sigma^{\frac{n}{2}}) = +1$ dès que 4 divise n. Ce qui prouve que $\wedge_{v,\chi}$ est nul dès que 4 divise n. Ainsi, sauf peut-être pour (P_2) dont l'étude est faite au paragraphe suivant, les conditions locales pour les places finies modérément ramifiées de K/k, sont automatiquement vérifiées.

III.4. Etude pour (P_2)

En remarquant que E_2 est alors cyclique d'ordre 4, on voit que l'on peut appliquer II théorème 1 qui nous dit qu'une condition nécessaire et suffisante pour que (P_2) admette une solution est que (-1) soit une norme locale pour toutes les places, donc une norme globale de K/k. Ceci justifie la partie du théorème 2 relative à (P_2).

III.5. Etude pour (P_4)

On commence par examiner l'injectivité de h, celle-ci étant acquise, (P_4) se réduit à l'étude des conditions locales ; cette étude est d'ailleurs déjà faite pour les places ne divisant pas 2 (en III.2. et III.3.).

a) Injectivité de h .

Si $K(\zeta)/k$ est de degré 2, Γ' est cyclique, donc Γ aussi et h est injective. Supposant $K(\zeta)$ de degré 4 sur k , $K(\zeta) = K' = k(\sqrt{-1},\sqrt{\alpha})$, on voit facilement que L est égal à $k(\sqrt{-\alpha})$ donc est cyclique de degré 2 sur k , ce qui prouve encore l'injectivité de h .

b) Etude des conditions locales pour les places au-dessus de 2 .

On distinguera trois cas :

1) $\alpha \notin \pm (k_v)^2$

Ainsi K_v/k_v est de degré 4. Il existe un élément $\tilde{\tau}$ de son groupe de Galois, laissant $\zeta = \sqrt{-1}$ invariant, mais pas α . Un caractère invariant par $\tilde{\tau}$ doit vérifier pour tout a de A_n :

$$\chi(a) = (\tilde{\tau}\chi)(a) = \chi^{-1}(a)$$

D'où $\chi(a) = \pm 1$.

Le même raisonnement que celui de III.3. montre que la condition locale est remplie.

2) $\alpha \in k_v^2$

G_v est alors trivial, les conditions locales sont vérifiées.

3) $\alpha \in -k_v^2 \qquad \alpha \notin k_v^2$

On peut faire le schéma suivant, représentant des extensions de k et leurs complétés :

$$\begin{array}{ccc} K' & \text{——} & K'_v = k_v(\sqrt{-1}) = k_v(\sqrt{\alpha}) \\ & & | \\ k(\sqrt{-\alpha}) & \text{———} & k_v \\ & \diagdown\!\!\diagup & \\ & k & \end{array}$$

Comme Γ'_v agit par symétrie sur les racines de l'unité et sur A_4 , il est clair que tous les caractères sont invariants. Etudions $\wedge_{v,\chi}$:

$$H^2(G,A) \xrightarrow{\sim} H^2(G_v,A) \xrightarrow{\simeq} H^2(\Gamma'_v,A) \to H^2(\Gamma'_v,K'_v) .$$

Comme Γ'_v est cyclique, on passe en dimension 0 :

$$\{1,\sigma^2\} = \hat{H}^0(\Gamma'_v,A) \to k_v^*/NK_v'^* = \hat{H}^0(\Gamma'_v,K'_v) .$$

Ainsi $\wedge_{v,\chi}$ est nul si, et seulement si, $\chi(\sigma^2)$ est une norme pour le caractère χ . Or, $\chi(\sigma^2)$ vaut $+1$ ou -1 . D'autre part, K'_v s'obtient en rajoutant $\sqrt{-1}$ à k_v . La condition locale est donc vérifiée si, et seulement si, le symbole de Hilbert $(-1,-1)_{k_v}$ vaut 1 , c'est-à-dire si le degré absolu de k_v est pair.

c) Conclusion.

Comme h est injective, les conditions locales sont nécessaires et suffisantes. Or, elles sont vérifiées, sauf peut-être pour les places finies au-dessus de 2, étudiées ci-dessus. Le théorème 2 est donc démontré pour la partie concernant (P_4) .

III.6. Etude pour (P_8)

Etudions d'abord les cas où K et $\mathbb{Q}(\zeta)$ ne sont pas linéairement disjoints (a et b) :

a) $K = k(\sqrt{-1})$

On observe que le corps L est égal à $k(\sqrt{2})$ donc est cyclique de degré 1 ou 2 sur k . L'application h est donc injective. Les conditions locales au-dessus de 2 sont donc nécessaires et suffisantes. Supposons d'abord que v soit telle que $\sqrt{2}$ ne soit pas dans k_v . Il existe alors dans Γ'_v un élément t opérant de la façon suivante sur les racines de l'unité :

$$\zeta^t = \zeta^5 .$$

Ainsi $\sqrt{-1}$ est invariant, donc t n'opère pas sur A . L'action sur les caractères est donc : $\chi^t = \chi^5$. Tout caractère invariant par Γ'_v a donc son image dans $\{\pm 1, \pm\sqrt{-1}\}$ donc dans K_v^* . L'application $\wedge_{v,\chi}$ se factorise alors :

$$H^2(G,A) \to H^2(G_v,A) \to H^2(G_v,K_v^*) \xrightarrow{\inf} H^2(\Gamma'_v,K_v'^*) .$$

L'application du milieu est nulle, car correspond en dimension 0 à :

$$A^{G_v} \xrightarrow{\chi} k_v^*/NK_v^* .$$

Si G_v est nul le dernier groupe est nul et c'est évident. Si G_v n'est pas nul, on a : $A^{G_v} = \{1, \sigma^4\}$ et $\chi(\sigma^4) = \chi^4(\sigma) = 1$ d'où la nullité de l'application considérée.

Supposons maintenant que $\sqrt{2}$ soit dans k_v. Tous les caractères sont invariants ; la situation ressemble à celle de III.5.b) 3), mais comme $\sqrt{2}$ est dans k_v le degré local est pair et la condition locale est remplie.

On voit donc que les conditions locales relatives à (P_8) sont toujours remplies, ce qui compte-tenu de l'injectivité de h signifie que (P_8) admet toujours une solution dans notre cas.

Remarque : puisque l'on suppose que la condition sur les places réelles est vérifiée, k désigne ici un corps de nombres totalement imaginaire.

b) Autres cas où K et $\mathbb{Q}(\zeta)$ ne sont pas linéairement disjoints.

Les sous-extensions quadratiques de $\mathbb{Q}(\zeta)$ étant engendrées par $\sqrt{2}$, $\sqrt{-2}$, $\sqrt{-1}$ les seuls cas possibles restants sont les suivants :

- $\sqrt{2} \in k$ ou $\sqrt{-2} \in k$ ou $\sqrt{-1} \in k$. Le degré local pour les places au-dessus de 2 est pair, donc les conditions locales pour (P_4) sont remplies (P_4) admettant une solution, d'après le théorème 1, il en est de même pour (P_8).

- $K = k(\sqrt{2})$ ou $K = k(\sqrt{-2})$. Soit $\alpha = \pm 2$ si $\alpha \in -(k_v)^2$ alors k_v contient $\mathbb{Q}_2(\sqrt{2})$ ou $\mathbb{Q}_2(\sqrt{-2})$ et le degré local est pair. Les conditions locales sont donc remplies : (P_4) et donc (P_8) admettent toujours une solution.

c) Cas où K et $\mathbb{Q}(\zeta)$ sont linéairement disjoints.

On va voir que dans ce cas h n'est pas forcément injective et que les conditions locales pour les places finies sont toujours toutes vérifiées. L'injectivité de h fournit donc une condition suffisante pour que (P_8) admette une solution : c'est celle du théorème 2.

1) Injectivité de h.

K et $\mathbb{Q}(\zeta)$ étant linéairement disjoints, Γ est engendré par trois générateurs d'ordre 2 :

- τ : laissant invariant les racines de l'unité, $\tau(\sqrt{\alpha}) = -\sqrt{\alpha}$.
- s tel que $s(\sqrt{\alpha}) = \sqrt{\alpha}$ et $s(\zeta) = \zeta^{-1}$.
- t tel que $t(\sqrt{\alpha}) = \sqrt{\alpha}$ et $t(\zeta) = \zeta^5$.

Ainsi pour tout caractère χ on a $\tau\chi = \chi^{-1} = s\chi$ et $t\chi = \chi^5$. Il est facile de voir que le groupe laissant fixe les caractères est $\{1, s\tau\}$. Le corps qui lui est associé est $L = k(\sqrt{2}, \sqrt{-\alpha})$.

On applique alors le théorème 2 du chapitre I : pour que h soit injective, il faut et il suffit qu'il existe une place v telle que $\Gamma_v = \Gamma$. Il est clair qu'une telle place est ramifiée. Dire que Γ est égal à Γ_v revient à dire qu'aucun des trois nombres 2, $-\alpha$, -2α n'est dans $(k_v)^2$.

2) Vérification des conditions locales.

On peut supposer v au-dessus de 2. On peut alors distinguer trois cas :

- $\Gamma'_v = \{1\}$
- $\Gamma'_v = \{1, s\tau\}$
- $\Gamma'_v \subsetneq \{1, s\tau\}$.

Dans le premier cas, il est clair que les applications $\wedge_{v,\chi}$ sont nulles pour χ dans $\tilde{A}_v$. Dans le second cas, on observe que le raisonnement ressemble à celui de III.5.b) 3), le degré local étant pair, car $\sqrt{2}$, invariant par $s\tau$, est dans k_v . Dans le troisième cas, on observe qu'il existe des caractères non invariants. On a donc $\tilde{A}_v \subsetneq \hat{A}$. Le groupe $\hat{A}$ étant cyclique d'ordre 8, on en déduit que les caractères dans $\tilde{A}_v$ vérifient $\chi^4 = 1$, le raisonnement se termine alors comme celui de III.6.a).

III.7. Cas où le corps k est celui des rationnels.

Traduisons le théorème 2 dans le cas où K/k est une extension quadratique $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$. On choisit m entier sans facteur carré. La condition sur la place réelle signifie que m doit être positif. La condition sur (P_4) signifie que $(-m)$ ne doit pas être un carré de $\mathbb{Q}_2$, ce qui s'exprime encore en disant que m ne doit pas être congru à -1 mod 8 .

Pour (P_8) on voit que l'on peut supposer m congru à -1 modulo 8 (car sinon (P_4) admet déjà une solution). Si v est la place correspondant à 2 , (-m) est donc alors dans $(k_v)^2$. Une place vérifiant la condition du théorème 2 correspondant donc à un diviseur premier p impair de m . Il est alors impossible que -m et -2m soient dans $(k_v)^2$. Tout revient donc à la non trivialité du symbole de Legendre

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} .$$

La condition suffisante est donc remplie lorsque m possède un facteur premier congru à ± 3 modulo 8.

On peut donc retrouver les premiers résultats de [3] :

Théorème 3.

Pour que l'extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ (m entier sans facteur carré) se plonge dans une surextension quaternionique sur $\mathbb{Q}$, il faut que m soit positif. Cette condition étant supposée réalisée, (P_2) admet une solution si, et seulement si, m est non congru à (-1) modulo 8 , (P_4) admet une solution si et seulement si m est congru à (-1) modulo 8 , (P_8) admet une solution si m possède un facteur premier congru à ±3 modulo 8 .

En fait comme le dit [3] la réciproque pour (P_8) est vérifiée. [3] donne aussi une condition suffisante pour que (P_n) admette une solution.

BIBLIOGRAPHIE

[1] - ARTIN-TATE - "Class Field Theory".

[2] - CASSELS-FROHLICH - "Algebraic Number Theory".

[3] - DAMEY - "Sur certaines 2-extensions galoisiennes, non abéliennes d'un corps de caractéristique différente de 2 ".

[4] - GILLARD - "Sur le problème des extensions galoisiennes". Compte-rendus de l'Académie des Sciences (à paraître).

[5] - HOECHSMANN - (J. für reine und ang. Math. 229 (1968) pp. 81-106).

[6] - POITOU - "Cohomologie galoisienne des modules finis" Dunod Paris.

[7] - RICHTER - (Math. Ann. 112 (1936) pp. 700-726).

[8] - SERRE - "Corps Locaux" Hermann Paris.
