ANNALES DE L'INSTITUT FOURIER

GEORGES POITOU

Conditions globales pour les problèmes de plongement à noyau abélien

Annales de l'institut Fourier, tome 29, n° 1 (1979), p. 1-14

<http://www.numdam.org/item?id=AIF_1979__29_1_1_0>

Ann. Inst. Fourier, Grenoble
29, 1 (1979), 1-14

CONDITIONS GLOBALES POUR LES PROBLÈMES DE PLONGEMENT A NOYAU ABÉLIEN

par Georges POITOU

Dédié à Monsieur Claude Chabauty.

L'introduction de la dualité dans l'étude des problèmes de plongement remonte à H. Hasse [5]. Traduite en langage cohomologique par K. Hoechsmann [6], son idée revient à constater que, pour qu'un problème de plongement à noyau abélien admette une solution, même en un certain sens faible, il est nécessaire que la 2-classe de cohomologie du problème soit annulée par les caractères du noyau, à valeurs dans le groupe multiplicatif, et définis sur le corps de base. Dans le cas des corps locaux, J. Neukirch [8] a remarqué que la dualité locale entraîne que ces conditions suffisent pour l'existence de solutions au sens faible. En outre, dans le cas des corps de nombres algébriques, il a déduit de la dualité globale une liste de cas où l'existence d'une solution (au sens faible ou au sens propre, c'est la même chose d'après M. Ikeda [7]) est assurée par l'existence de solutions faibles pour les problèmes locaux correspondants, existence qui n'est d'ailleurs en cause que pour un nombre fini de places. Dans le cas général, on peut tirer de la dualité globale un système de conditions, nécessaire et suffisant pour l'existence d'une solution à un problème de plongement à noyau abélien, portant sur des corps de nombres algébriques. Ces conditions comprennent les conditions locales précédentes, essentiellement en nombre fini, et en outre un nombre fini de conditions dites *globales*. Celles-ci sont obtenues en annulant la 2-classe de cohomologie du problème par des caractères du noyau, définis sur le corps de base, et prenant leurs valeurs dans des groupes de classes d'idèles. Par exemple, lorsque le noyau est cyclique, il y a au plus une condition globale ; son écriture est complètement explicite si l'extension de base est elle-même cyclique.

1.

Rappelons qu'un problème de plongement à noyau abélien comporte les données suivantes : Une extension galoisienne K/k, un module A sur le groupe de Galois G de K/k, un type d'extension $\epsilon \in H^2(G, A)$. Ce problème est noté $(K/k, A, \epsilon)$. Une solution est une surextension L/k galoisienne dont le groupe de Galois réalise l'extension donnée de G par A (en particulier, l'extension L/K est galoisienne de groupe A). Une telle solution est dite propre ; on considère aussi des solutions faibles, qui ne sont plus forcément des corps, mais des algèbres galoisiennes au sens de Hasse [5] ; cf. K. Hoechsmann [6]. D'après ce dernier, l'existence d'une solution faible est caractérisée par la nullité de l'image de ϵ par inflation dans le groupe $H^2(\mathfrak{G}, A)$, où $\mathfrak{G}$ est le groupe de Galois d'une clôture séparable de k. Dans le cas des corps de nombres algébriques (mais non pour les corps locaux) l'existence de solutions faibles entraîne celle de solutions propres, d'après un théorème d'Ikeda [7] ; cf. J. Neukirch [8] Korollar 6.7. C'est cette condition $\inf(\epsilon) = 0$ qui, dans le cas local, est transcrite par J. Neukirch [8] en termes d'extensions finies à partir des caractères $\chi : A \longrightarrow \bar{k}^\times$ définis sur k ; il faut et il suffit que s'annulent, dans $H^2(G, K^\times)$, toutes les images $\chi^*(\epsilon)$.

Procédons de même dans le cas global en remplaçant le groupe multiplicatif par le groupe des classes d'idèles. Soit $\mathcal{C}$ la limite inductive des groupes des classes d'idèles des extensions finies de k. Comme l'on sait, les groupes H^1 des classes d'idèles sont nuls (cf. Artin-Tate [1]) ; c'est là une forme du théorème de Hasse sur les algèbres. De là, et de la suite exacte de Hochschild-Serre, résulte l'injectivité de l'inflation $H^2(G, \mathcal{C}_K) \longrightarrow H^2(\mathfrak{G}, \mathcal{C})$. Soit $\chi : A \longrightarrow \mathcal{C}$ un caractère défini sur k, donc invariant par $\mathfrak{G}$ vis-à-vis de l'opération habituelle $(g\chi)(a) = g(\chi(g^{-1}a))$. En particulier, les valeurs de χ sont dans $\mathcal{C}_K$. Ce caractère transporte ϵ dans un élément $\chi^*(\epsilon)$ du groupe $H^2(G, \mathcal{C}_K)$, qui doit donc être nul pour que $\inf(\epsilon)$ le soit.

Inversement, je dis que la nullité de $\inf(\epsilon)$ résulte de celle des éléments $\chi^*(\epsilon)$ pour tous les caractères χ de $\mathrm{Hom}_k(A, \mathcal{C}) = H^0(\mathfrak{G}, \mathrm{Hom}(A, \mathcal{C}))$ grâce à la dualité globale [10]. En effet, en dualité exacte avec le groupe $H^2(G, A)$ se trouve un

certain quotient de ce groupe H^0 (en fait le quotient par le groupe $N_{K/k}\,\mathrm{Hom}(A, \mathcal{D}_K)$, où $\mathcal{D}_K$ est le groupe des normes universelles des classes d'idèles pour le corps K).

Je dis maintenant qu'il suffit d'écrire les conditions $\chi^*(\epsilon) = 0$ pour un nombre fini de caractères χ, si l'on a déjà exprimé les conditions locales (elles-mêmes en nombre fini). Soit en effet $\mathcal{J}$ la limite inductive des groupes d'idèles des extensions finies de k, et $\pi : \mathcal{J} \longrightarrow \mathcal{C}$ la projection canonique, dont le noyau est le groupe $\bar{k}^\times$ (groupe multiplicatif de la clôture algébrique $\bar{k}$ de k). Une suite exacte de cohomologie nous montre que le conoyau de la flèche $\pi^* : \mathrm{Hom}_k(A, \mathcal{J}) \longrightarrow \mathrm{Hom}_k(A, \mathcal{C})$ est aussi le noyau de la flèche $H^1(k, \mathrm{Hom}(A, \bar{k}^\times)) \longrightarrow H^1(k, \mathrm{Hom}(A, \mathcal{J}))$ ou encore le noyau de la flèche $\rho : H^1(k, \mathrm{Hom}(A, \bar{k}^\times)) \longrightarrow \prod_v H^1(k_v, \mathrm{Hom}(A, \bar{k}_v))$ (en effet, on sait que le groupe $H^1(k, \mathrm{Hom}(A, \mathcal{J}))$ est un certain produit restreint, sous-groupe du produit ci-dessus ; quant à la flèche ρ, c'est le produit des restrictions, si on considère le groupe de Galois au-dessus de k_v comme un sous-groupe de décomposition du groupe $\mathfrak{G}$ relativement à un prolongement de v). Ce noyau, on le sait, est fini. Les cas où il est nul sont justement ceux, signalés par J. Neukirch, où les conditions locales suffisent. Dans le cas général, notre assertion de finitude résulte de la remarque que, lorsque le caractère χ est dans l'image de π^*, les conditions $\chi^*(\epsilon) = 0$ résultent des conditions locales. En effet, s'il existe un élément ψ de $\mathrm{Hom}_k(A, \mathcal{J})$ tel que $\chi = \pi^*(\psi)$, il se décompose selon les places v de k en morceaux $\psi_v : A \longrightarrow \prod_{w|v} K_w^\times$. Choisissons un prolongement w de v à K et désignons par φ_w le caractère composé de ψ_v et de la projection du produit ci-dessus sur le facteur $K_w^\times$; le caractère est fixé par le sous-groupe de décomposition G_w du groupe G. Si ϵ_w désigne la restriction de ϵ à G_w, on voit que les éléments $\varphi_w^*(\epsilon_w)$ et $\psi_v^*(\epsilon)$ se correspondent par l'isomorphisme de Shapiro (obtenu par restriction et projection) : $H^2(G, \prod_{w|v} K_w^\times) \longrightarrow H^2(G_w, K_w^\times)$. Donc la nullité de $\psi^*(\epsilon)$, et a fortiori de $\chi^*(\epsilon)$, résulte des conditions locales $\varphi_w^*(\epsilon_w) = 0$.

Quant à la finitude du noyau de ρ, elle résulte de la remarque que ce noyau est nul dans le cas où le module $A' = \mathrm{Hom}_{\mathbf{Z}}(A, \bar{k}^\times)$ est défini sur k ; dans ce cas, en effet, les 1-classes de cohomologie deviennent des homomorphismes continus, et on sait que les groupes de Galois sont engendrés par leurs sous-groupes de décomposition.

Donc les classes du noyau de ρ sont en fait dans le groupe $H^1(k(A')/k, A')$, qui est fini. Plus précisément, le noyau de ρ est égal à celui de l'application $\rho' : H^1(G', A') \longrightarrow \prod_{v'} H^1(G'_{v'}, A')$ où G' désigne le groupe de Galois de $k(A')/k$, et $G'_{v'}$ le sous-groupe de décomposition d'une place v' de $k(A')$.

Dans la pratique, on peut souvent pousser la réduction plus loin, et nous désignerons par k'/k une sous-extension galoisienne de $k(A')/k$, avec groupe de Galois Γ', telle que le noyau de ρ' provienne par inflation du noyau de $\rho'' : H^1(\Gamma', A'(k')) \longrightarrow \prod_{v'} H^1(\Gamma'_{v'}, A'(k'))$ (où $\Gamma'_{v'}$ désigne le sous-groupe de décomposition d'une place v' de k'). Il en est ainsi, par exemple, si le groupe G' possède un sous-groupe distingué cyclique D ; en effet, les sous-groupes cycliques sont des groupes de décomposition ; dans ce cas, il suffit de prendre pour k' le corps fixe par D dans $k(A')$. Dans le cas général, nous conservons ces notations, quitte à admettre, au pis, que $k' = k(A')$.

Complétons ces considérations générales en indiquant comment calculer, à partir des cocycles du noyau de ρ'', un système de représentants du groupe $\mathrm{Hom}_k(A, \mathcal{C})$ modulo l'image de l'application π^*.

Soit (a'_σ) un cocycle du noyau de ρ'' ; par hypothèse, il dégénère sur tout sous-groupe de décomposition $\Gamma'_{v'}$. Comme on l'a dit plus haut, cette condition s'exprime aussi par l'existence d'un élément ψ du groupe $\mathrm{Hom}_{k'}(A, \mathcal{J})$ vérifiant (pour $\sigma \in \Gamma'$) les équations

$$a'_\sigma = \psi / {}^\sigma\psi \ . \tag{1}$$

Par composition avec $\pi : \mathcal{J} \longrightarrow \mathcal{C}$, on obtient un élément χ qui appartient à $\mathrm{Hom}_k(A, \mathcal{C})$, mais non à l'image de π^*, si le cocycle donné (a'_σ) n'est pas un cobord. Il s'agit donc de résoudre les équations (1) pour chaque donnée d'un cocycle représentant une classe non nulle du noyau de ρ'' (ou même en se limitant à un système de générateurs de ce noyau). Pour cela, on procède localement pour chaque place v de k, et on cherche à résoudre les équations

$$a'_\sigma = \psi_v / {}^\sigma\psi_v \tag{2}$$

avec ψ_v dans le groupe $\mathrm{Hom}_{k'}(A, \mathcal{J}_v)$; ici $\mathcal{J}_v$ désigne la composante de $\mathcal{J}$ au-dessus de v, c'est-à-dire la limite inductive des produits $\prod_{x|v} L_x^\times$, où L décrit les extensions finies de k. Ce groupe

$\mathrm{Hom}_{k'}(A, \mathcal{J}_v)$ se calcule déjà dans l'extension Kk'/k sous la forme $\mathrm{Hom}_{k'}(A, \prod_{w'|v} (Kk')^{\times}_{w'})$.

LEMME. – *Le module* $\mathrm{Hom}_{k'}(A, \mathcal{J}_v)$ *sur le groupe* Γ' *est induit par le module* $\mathrm{Hom}_{k'_{v'}}(A, \overline{k}_v^{\times})$ *sur le groupe* $\mathrm{Gal}(k'_{v'}/k_v)$, *identifié au sous-groupe de décomposition* $\Gamma'_{v'}$.

Preuve. – Il est bien connu que le module $\prod_{w'|v} (Kk')^{\times}_{w'}$ sur le groupe $G = \mathrm{Gal}(Kk'/k)$ est induit par le module $(Kk')^{\times}_{w'}$ sur le groupe F de décomposition de w'. Il en est donc de même pour le G-module $\mathrm{Hom}_{\mathbf{Z}}(A, \prod_{w'|v} (Kk')^{\times}_{w'})$ et le F-module $X = \mathrm{Hom}_{\mathbf{Z}}(A, (Kk')^{\times}_{w'})$. Soit maintenant U le sous-groupe distingué de G qui fixe k' ; alors $F / F \cap U$ est un sous-groupe de $G/U = \Gamma'$, et c'est le sous-groupe de décomposition de la place v' de k' au-dessous de w'. Le lemme est alors une conséquence de la formule suivante, dans les notations de Serre [9] :

$$H^0(U, M_G^F X) = M_{G/U}^{F/F\cap U} (X^{F\cap U}).$$

Ainsi, par le lemme, le groupe $\mathrm{Hom}_{k'}(A, \mathcal{J}_v)$ est identifié à la somme directe (pour les $v'|v$) des groupes $\mathrm{Hom}_{k'_{v'}}(A, \overline{k}_v^{\times})$ que l'on notera encore $A'(k'_{v'})$. Donc un élément $\psi_v \in \mathrm{Hom}_{k'}(A, \mathcal{J}_v)$ se représente par une famille $(\varphi_{v'})_{v'|v}$, avec $\varphi_{v'} \in A'(k'_{v'})$. Quant à l'opération d'un élément σ du groupe Γ', elle se décrit ainsi :

Prolongeons σ à Kk', et notons w' une place de Kk' au-dessus de v'. Alors l'isomorphisme habituel $\sigma_{w'} : (Kk')_{w'} \longrightarrow (Kk')_{\sigma w'}$ en induit un autre $\sigma^*_{w'} : \mathrm{Hom}_{\mathbf{Z}}(A, (Kk')^{\times}_{w'}) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(A, (Kk')^{\times}_{\sigma w'})$ défini par la formule $\sigma^*_{w'}(\varphi)(a) = \sigma_{w'}(\varphi(\sigma^{-1}a))$, avec une restriction bien définie $\sigma^*_{v'} : A'(k'_{v'}) \longrightarrow A'(k'_{\sigma v'})$ et l'on a donc, en posant $\sigma((\varphi_{v'})_{v'|v}) = (\varphi'_{v'})_{v'|v}$, les formules $\varphi'_{\sigma v'} = \sigma^*_{v'}(\varphi_{v'})$ ou encore $\sigma((\varphi_{\sigma v'})_{v'|v}) = (\sigma^*_{v'}(\varphi_{v'}))_{v'|v}$ de sorte que les équations (2) prennent la forme

$$a'_\sigma = \varphi_{\sigma v'} / \sigma^*_{v'}(\varphi_{v'}). \tag{3}$$

Par hypothèse, si σ décrit seulement le groupe de décomposition d'une place v'_0 au-dessus de v, ces équations ont une solution, donc il existe une fonction $\varphi_{v'_0} \in A'(k'_{v'_0})$ telle que (pour $\sigma v'_0 = v'_0$) on ait

$$a'_\sigma = \varphi_{v'_0} / \sigma^*_{v'_0}(\varphi_{v'_0}). \tag{4}$$

On voit alors que l'on obtient une solution de (3) en posant $\varphi_{v'} = a'_\sigma \, \sigma^*_{v'_0}(\varphi_{v'_0})$, où σ envoie v'_0 sur v' ; en effet l'identité des cocycles assure que φ'_v ne dépend pas du choix de σ, puisque la famille $(\varphi_{v'})_{v'|v}$ est une solution de (3).

Remarque. – Les assertions de finitude et la méthode ci-dessus s'étendent à un problème de plongement $(K/k, A, \epsilon, S)$ avec ramification limitée à un ensemble S de places de k, contenant les diviseurs du cardinal de A et les places déjà ramifiées dans K/k ; en effet la dualité globale est encore valable ([10], [11]).

2. Cas particulier où A est cyclique.

On se réduit facilement au cas où l'ordre m de A est de la forme p^r, où p est un nombre premier. Il en est de même pour le groupe dual $A' = \mathrm{Hom}(A, \bar{k}^X)$ et il est alors bien connu que l'application $\rho : H^1(k, A') \longrightarrow \prod_v H^1(k_v, A')$ est injective, sauf dans un cas très particulier qui va maintenant nous occuper, et qu'on peut décrire ainsi : l'extension $k(A')/k$ n'est pas cyclique, mais son groupe de Galois diffère de tous les groupes de décomposition (en particulier, on a forcément $p = 2$, $m \geqslant 8$). Du moins ceci est-il analysé en détail dans les notes d'Artin-Tate [1] pour le cas où A' est le module des racines m-ièmes de l'unité (c.a.d. où A est un module trivial) ; mais ces raisonnements contiennent aussi le cas général, si on leur donne la forme d'un lemme élémentaire sur la cohomologie :

PROPOSITION. – *Soit* C *un groupe cyclique d'ordre* $2^r \geqslant 8$, *et* Δ *un groupe d'automorphismes de* C, *considéré comme sous-groupe de* $(\mathbf{Z}/2^r\mathbf{Z})^\times$. *Alors 1) le groupe* $H^1(\Delta, C)$ *a deux éléments ou bien un seul, selon que* Δ *contient* -1 *ou non ; 2) le groupe* $H^1(\Delta, C)$ *s'annule par restriction à un sous-groupe propre de* Δ.

Preuve. – a) liste des sous-groupes de $\Gamma = (\mathbf{Z}/2^r\mathbf{Z})^\times$ pour $r \geqslant 3$. Soient $\alpha = 5$ et $\beta = -1$ les générateurs de Γ. Les sous-groupes du groupe cyclique (α) sont les suivants :

$$\Delta_0 = (\alpha) \quad \Delta_1 = (\alpha^2) \ldots \Delta_{r-3} = (\alpha^{2^{r-3}}) \quad \Delta_{r-2} = \{1\}.$$

Par adjonction de $\beta = -1$, on obtient des sous-groupes contenant -1 :

$$\Delta'_0 = \Gamma \quad \Delta'_1 = (-1, \alpha^2) \ldots \Delta'_{r-3} = (-1, \alpha^{2^{r-3}}) \quad \Delta'_{r-2} = (-1).$$

Les autres sous-groupes sont les suivants :

$$\Delta_0^- = (-\alpha) \quad \Delta_1^- = (-\alpha^2) \ldots \Delta_{r-3}^- = (-\alpha^{2^{r-3}}).$$

b) nullité de $H^1(\Delta, C)$ pour $\Delta = \Delta_s$ ou Δ_s^- : elle résulte d'un calcul bien classique s'appuyant sur la congruence $5^{2^j} \equiv 1 + 2^{j+2} \bmod 2^{j+3}$. Soit $\alpha' = \pm\alpha^{2^s}$ un générateur de Δ, avec $0 \leqslant s \leqslant r-3$. La somme des conjugués par Δ d'un élément x de C se calcule comme

$$N_\Delta x = x + \alpha' x + \alpha'^2 x + \ldots + \alpha'^{2^{r-2-s}-1} x = \frac{\alpha'^{2^{r-2-s}} - 1}{\alpha' - 1} x.$$

Comme $\alpha'^{2^{r-2-s}} - 1$ est exactement divisible par 2^r, les x tels $N_\Delta x = 0$ sont exactement ceux de la forme $x = (1-\alpha')y$, ce qui prouve la nullité de $H^1(\Delta, C)$.

c) calcul de $H^1(\Delta'_s, C)$ pour $0 \leqslant s \leqslant r-2$. Comme on a $H^1(\Delta_s, C) = 0$, le groupe en question est égal à

$$H^1((\beta), C^{\Delta_s}) = C^{\Delta_s}/(C^{\Delta_s})^2 = C_{2^{s+2}}/C_{2^{s+1}}$$

qui est d'ordre deux.

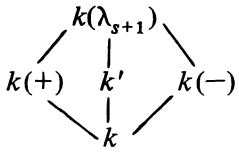
d) restriction à un sous-groupe propre. Il suffit d'examiner la flèche res : $H^1(\Delta'_s, C) \longrightarrow H^1(\Delta'_{s+1}, C)$; or c'est la flèche naturelle de $C_{2^{s+2}}/C_{2^{s+1}}$ dans $C_{2^{s+3}}/C_{2^{s+2}}$, et elle est donc nulle.

Pour représenter l'unique classe non nulle de $H^1(\Delta'_s, C)$, désignons par λ_s un élément d'ordre 2^{s+2} de C, choisi de façon que $\lambda_{s+1}^2 = \lambda_s$; on peut alors choisir le cocycle qui prend, sur le sous-groupe Δ_s, la valeur 1_C, et sur la classe de -1 modulo Δ_s, la valeur λ_s. Conservons ces notations pour l'application au cas où C est le groupe A'.

Dans ce cas, le groupe $G' = \mathrm{Gal}(k(A')/k)$ est un certain sous-groupe du groupe $\Gamma = (\mathbf{Z}/2^r\mathbf{Z})^\times$. Comme ci-dessus le noyau de l'application $\rho : H^1(k, A') \longrightarrow \prod_v H^1(k_v, A')$ coïncide avec celui de l'application $\rho' : H^1(G', A') \longrightarrow \prod_v H^1(G'_{v'}, A')$. Si ce noyau n'est pas nul, alors tous les groupes $G'_{v'}$ diffèrent de G', et ceci

implique que G' n'est pas cyclique, puisque les sous-groupes cycliques sont des groupes de décomposition ; donc il existe un entier s compris entre 0 et $r-3$, tel que $G' = \Delta'_s$.

Inversement, si $G' = \Delta'_s$ et si aucun $G'_{v'}$ n'est égal à G', alors le noyau de ρ' possède deux éléments. L'élément non nul est décrit par un cocycle à deux valeurs $(1, \lambda_s)$ (ici 1 désigne l'unité de A', c'est le caractère partout égal à 1). Notons k' le corps $k(\lambda_s) = k(A'^{\Delta_s})$, qui est quadratique sur k, et $\overline{\beta}$ le générateur de son groupe de Galois. On a $\overline{\beta}(\lambda_s) = \lambda_s^{-1}$. En particulier, $\lambda_s + \lambda_s^{-1}$ est défini sur k, et ceci détermine s, car $\lambda_{s+1} + \lambda_{s+1}^{-1}$ n'est pas défini sur k. En fait, $k(A')$ contient trois sous-corps quadratiques, fixés par les sous-groupes Δ_s, Δ'_{s+1}, Δ_s^-, et contenus dans un corps biquadratique fixé par le sous-groupe Δ_{s+1}, et engendré par λ_{s+1}. Le groupe de Galois de $k(\lambda_{s+1})/k$ est engendré par -1 et 5^{2^s} ; d'après la congruence ci-dessus, l'effet de 5^{2^s} sur λ_{s+1} est l'élévation à la puissance $1 + 2^{s+2}$, et le résultat est le produit $\lambda_{-1}\lambda_{s+1}$ (λ_{-1} est le caractère égal à -1 sur un générateur de A). Le corps fixe par Δ_s, ou par 5^{2^s}, est $k(\lambda_s) = k'$; celui fixe par Δ'_{s+1}, ou par -1, est $k(\lambda_{s+1} + \lambda_{s+1}^{-1})$, en abrégé $k(+)$; celui fixe par Δ_s^-, ou par -5^{2^s}, est $k(\lambda_{s+1} + \lambda_{-1}\lambda_{s+1}^{-1})$, en abrégé $k(-)$.



Par hypothèse, toute place de k se décompose au moins dans l'un de ces corps.

Calculons maintenant le caractère $\psi \in \mathrm{Hom}_{k'}(A, \mathcal{J})$ associé au cocycle crucial $(1, \lambda_s)$ du groupe $H^1(k'/k, A'(k'))$. D'après la méthode générale de calcul de la composante locale ψ_v, il y a lieu de distinguer deux cas :

Premier cas. — Le sous-groupe de décomposition est nul : la place v possède dans k' deux prolongements v' et v''. La composante ψ_v est représentée par un couple $(\varphi_{v'}, \varphi_{v''})$ avec $\varphi_{v'} \in A'(k'_{v'})$ et $\varphi_{v''} \in A'(k'_{v''})$, l'opération de $\overline{\beta}$ étant donnée par $\overline{\beta}(\varphi_{v'}, \varphi_{v''}) = (\overline{\beta}^*_{v'',v'}(\varphi_{v''}), \overline{\beta}^*_{v'}(\varphi^*_{v'}))$. L'équation à vérifier se réduit

d'après (3) à $\lambda_s = \varphi_{v''}/\overline{\beta}_{v'}^*(\varphi_{v'})$ et se résoud (conformément à (4)) par le choix (par exemple) $\varphi_{v''} = \lambda_s$, $\varphi_{v'} = 1$.

Deuxième cas. – Le sous-groupe de décomposition est le groupe Γ' entier : il existe dans k' une seule place au-dessus de v, que nous notons encore v. Le module $\mathrm{Hom}_{k'}(A, \mathcal{J}_v)$ s'identifie à $A'(k_v')$. Notons φ_v l'image de ψ_v par cette identification. Les équations (3) se réduisent à

$$\lambda_s = \varphi_v/\overline{\beta}_v^*(\varphi_v). \tag{5}$$

Dans ce deuxième cas, λ_{s+1} est défini sur k_v', et selon que $\lambda_{s+1} + \lambda_{s+1}^{-1}$ ou $\lambda_{s+1} + \lambda_{-1}\lambda_{s+1}^{-1}$ est défini sur k_v, on a $\overline{\beta}_v^*(\lambda_{s+1}) = \lambda_{s+1}^{-1}$ ou $\lambda_{-1}\lambda_{s+1}^{-1}$. Comme solution de l'équation (5) on peut alors prendre respectivement $\varphi_v = \lambda_{s+1}$ ou $\varphi_v = \lambda_0\lambda_{s+1}$.

Désignons par ψ l'élément de $\mathrm{Hom}_{k'}(A, \mathcal{J})$ ainsi choisi localement, et par $\overline{\psi}$ son image dans $\mathrm{Hom}_k(A, \mathcal{C})$. Par cet élément $\overline{\psi}$, la classe de cohomologie $\epsilon \in H^2(G, A)$ est transportée dans une classe $\overline{\psi}^*(\epsilon) \in H^2(G, \mathcal{C}(K))$, autrement dit donne un certain nombre rationnel modulo 1, annulé par le degré $[K : k]$; et la nullité de cette obstruction est nécessaire et suffisante, une fois les conditions locales remplies, pour que le problème de plongement $(K/k, A, \epsilon)$ admette une solution. Ce qu'ont peut énoncer ainsi :

THEOREME. – *Soit* $(K/k, A, \epsilon)$ *un problème de plongement dont le noyau* A *est cyclique. On suppose que les problèmes locaux correspondants ont des solutions faibles, et on se place dans le cas suivant (sinon, le problème donné est toujours résoluble) : En désignant par* A' *le module dual de* A, *l'extension* $k(A')/k$ *a un groupe de Galois non cyclique, et distinct de tous ses groupes de décomposition. On considère le caractère* $\overline{\psi} : A \longrightarrow \mathcal{C}(K)$ *construit ci-dessus, qui est invariant par le groupe de Galois* G *de l'extension* K/k. *Alors, pour que le problème posé admette une solution, il faut et il suffit que l'invariant* $\overline{\psi}^*(\epsilon)$ *dans* $H^2(G, \mathcal{C}(K)) = (\mathbf{Q}/\mathbf{Z})_{[K:k]}$ *soit nul.*

Remarque. – Le fait que le noyau de ρ soit d'ordre 1 ou 2 quand A est cyclique subsiste même si on exclut du produit des groupes $H^1(k_v, A')$, disons un nombre fini S de places v. Or, le quotient de ce nouveau noyau par l'ancien représente, d'après

J. Neukirch [8], l'obstruction pour imposer au problème $(K/k, A, \epsilon)$, supposé résoluble, le comportement local des solutions aux places de S. Comme cette obstruction est nulle si le noyau de ρ ne l'est pas, on obtient alors un prolongement au "cas spécial" du théorème 6.6 de [8] (généralisation du théorème de Grunwald-Wang).

3. Cas plus particulier où G aussi est cyclique.

Dans ce cas, le groupe $H^2(G, A)$ s'identifie à $A^G/N_G A$, et l'invariant ϵ provient d'un certain élément a_ϵ de A^G. La classe de cohomologie $\overline{\psi}^*(\epsilon)$ s'exprime alors à partir de la classe d'idèles $\overline{\psi}(a_\epsilon) \in \mathcal{C}(k)$ comme sa classe dans le quotient $\mathcal{C}(k)/N_{K/k}\,\mathcal{C}(K)$. On doit donc exprimer que cette classe d'idèles est une norme ; pour cela, en la représentant par un idèle (y_v) de k, on écrit au moyen des invariants locaux $\sum_v (y_v, K/k)_v = 0$ où la somme est, comme d'habitude, essentiellement finie.

L'accomplissement de ce programme demande quelques notations.

Le cardinal de A étant toujours 2^r, désignons par 2^d celui de A^G. Soit τ un générateur du groupe cyclique G, et u l'entier impair modulo 2^r, tel que $\tau(a) = a^u$ pour $a \in A$. Cet entier u s'écrit $(-1)^w\, 5^{(2^t)i}$ avec i impair, $w = 0$ ou 1 et $0 \leqslant t \leqslant r-2$. Pour qu'un élément de A soit fixe par G, il faut et il suffit qu'il soit annulé par $u-1$, donc l'ordre 2^d de A^G est égal au pgcd de $u-1$ et de 2^r, et d est donné par :

$$\text{si} \quad w = 1 \quad \text{alors} \quad d = 1$$

$$\text{si} \quad w = 0 \quad \text{alors} \quad d = t + 2.$$

Ainsi, on a $A^G = A_{2^d} = A^{2^{r-d}}$, et a_ϵ est une puissance 2^{r-d}-ième dans A. Ecrivons donc $a_\epsilon = a^{2^m}$, où a engendre A, avec $m \geqslant r-d$. Ainsi $\overline{\psi}(a_\epsilon) = \overline{\psi}(a)^{2^m}$ est décrit localement par des racines de l'unité d'ordre divisant 2^{s+3-m}. Désignons par ζ celle, qui a précisément cet ordre 2^{s+3-m}, donnée par la formule $\zeta = \lambda_{s+1}(a^{2^m}) = \lambda_{s+1-m}(a)$, ceci, pourvu que l'on ait $s+3-m \geqslant 0$; mais si $s+3-m$ est négatif (ou nul), ζ est égale à 1 et la condition globale s'évanouit. Ainsi, la classe d'idèles $\overline{\psi}(a_\epsilon)$ est définie par l'idèle $z = (z_{v'})$ de k' décrit comme suit :

Cas I : places v de k décomposées dans k' en v' et v''. Les deux composantes $z_{v'}$ et $z_{v''}$ sont 1 et ζ^2.

Cas II : places v de k non décomposées dans k'. La composante z_v est ζ ou $i^{2^m}\zeta$ (où $i = \lambda_0(a) = \sqrt{-1}$) selon que $\lambda_{s+1} + \lambda_{s+1}^{-1}$ ou $\lambda_{s+1} + \lambda_{-1}\lambda_{s+1}^{-1}$ est défini sur k_v'.

Pour obtenir un idèle $y = (y_v)$ de k qui soit dans la même classe que z, il faut diviser z par un nombre convenable de k'. Ce nombre ω doit vérifier les deux conditions suivantes, relatives aux deux formes du cas II :

$$\beta\omega/\omega = \beta\zeta/\zeta = \zeta^{-2}$$

$$\beta\alpha^{2^s}(\omega)/\omega = \beta\alpha^{2^s}(i^{2^{r-d}}\zeta)/\, i^{2^{r-d}}\zeta$$

mais ces conditions sont équivalentes en vertu de $\alpha^{2^s}(\omega) = \omega$. Donc il suffit de résoudre dans k' l'unique équation $\beta\omega/\omega = \zeta^{-2}$ (on aura remarqué que ζ^2 se trouve bien dans k').

Une solution de cette équation est fournie par $\omega = 1 + \zeta^2$, pourvu que ce nombre soit non nul. S'il est nul, c'est-à-dire si $s + 3 - m = 2$, on peut prendre $\omega = \zeta(= i)$. Bien sûr, si $s + 3 - m = 1$, c'est-à-dire $\zeta = -1$, on peut se contenter de prendre $\omega = 1$, mais nous choisissons plutôt $\omega = -1$.

Avant d'écrire la condition globale explicitement, remarquons que les conditions locales en la place v disent que, pour tout caractère $\chi : A \longrightarrow \bar{k}_v^{\times}$, défini sur k_v, $\chi(A^{G_w})$ est contenu dans $N_{K_w/k_v} K_w^{\times}$; compte-tenu de l'inclusion de A^G dans A^{G_w}, il en résulte que l'on a $(\zeta^2, K/k)_v = 0$ si λ_s est défini sur k_v (c'est le cas I) et même $(\zeta, K/k)_v = 0$ si λ_{s+1} est défini sur k_v. Ces remarques lèvent les ambiguïtés apparentes des formules ci-dessous. On notera IIa resp. IIb les deux sous-cas du cas II, où $\lambda_{s+1} + \lambda_{s+1}^{-1}$ resp. $\lambda_{s+1} + \lambda_{-1}^{-1}\lambda_{s+1}^{-1}$ est défini sur k_v.

Rappelons qu'il n'y a à écrire de condition globale que si l'on a $s \leqslant r - 3$ et $s + 3 - m \geqslant 1$, et que l'on a $m \geqslant r - d$. Distinguons alors trois cas :

(1) $s + 3 - m \geqslant 3$.

Les inégalités $r - d \leqslant m \leqslant s \leqslant r - 3$ montrent que l'on a nécessairement $d \geqslant 3$, donc $w = 0$ et $t \geqslant 1$ (c'est dire que u est une puissance de 25, ou encore $u = 1$, ce qui est le cas de l'opération triviale). La condition globale s'écrit alors

$$0 = \sum_{\mathrm{I}} (1+\zeta^2, \mathrm{K}/k)_v + \sum_{\mathrm{II}a} (\zeta+\zeta^{-1}, \mathrm{K}/k)_v + \sum_{\mathrm{II}b} (i^{-2^m}\ (\zeta+\zeta^{-1}), \mathrm{K}/k)_v .$$

(2) $s + 3 - m = 2$.

On a alors $r - d \leqslant m = s + 1 \leqslant r - 2$, donc $d \geqslant 2$, donc $w = 0$ (ce qui signifie que u est égal à 1 ou à une puissance de 5). La condition globale s'écrit alors, compte-tenu des remarques locales :

$$0 = \sum_{\mathrm{II}a} (i, \mathrm{K}/k)_v + \sum_{\mathrm{II}b} ((-1)^{2^s} i, \mathrm{K}/k)_v .$$

(3) $s + 3 - m = 1$.

Ceci n'exclut aucune possibilité pour l'opération de G sur A. La condition globale s'écrit, au choix, sous l'une des deux formes suivantes :

$$0 = \sum_{\mathrm{II}} (-1, \mathrm{K}/k)_v$$

$$0 = \sum_{\mathrm{I}} (-1, \mathrm{K}/k)_v .$$

Bien entendu, dans les trois cas, les seules places v qui interviennent dans la sommation sont celles qui sont ramifiées dans K/k, et en outre, dans le cas (1), celles qui divisent 2.

Cas déjà connus. – Parmi les cas où G et A sont cycliques, deux ont été étudiés en détail :

1) Le cas où l'extension cherchée L/k est elle-même cyclique, cf. [1] § X, 3. Ce cas rentre dans celui de l'opération triviale de G sur A, pour lequel on a $d = r$; le corps $k(\mathrm{A}')$ est alors le corps des racines 2^r-ièmes de l'unité, et, pour qu'il y ait à écrire une condition globale, il est nécessaire qu'il soit une extension non-cyclique de k, avec des groupes de décomposition distincts du groupe de Galois. Ceci étant, il y aura effectivement une condition globale si l'on a l'inégalité $m \leqslant s + 2$, et c'est le cas pour une extension L/k cyclique, où $m = 0$.

2) Le cas tout à fait opposé de l'opération fidèle ne fournit d'extension non décomposée (donc de problème) que si l'extension L/k est quaternionienne, l'extension donnée K/k étant quadratique, avec τ opérant comme -1. Ici, on a $d = 1$, donc $m = r - 1$

et $s = r + 3$, donc la condition globale éventuelle est du type (3). En écrivant $K = k(\sqrt{b})$, on trouve que $k' = k(\sqrt{-b})$, et les places du type I sont celles pour lesquelles $-b$ est un carré localement. Pour une telle place v, on a donc

$$(-1, K/k)_v = (-1, b)_{k_v} = (-1, -1)_{k_v}$$

et ceci est nul si la place v ne divise pas 2, et vaut $(-1)^{n_v}$ si v divise 2, où n_v est le degré du corps k_v sur le corps $\mathbf{Q}_2$. Donc la condition globale s'exprime par le fait que le nombre de places v divisant 2, avec un degré local impair sur $\mathbf{Q}_2$, et pour lesquelles $-b$ est un carré, est un nombre pair. Cette condition disparaît si 2 est un carré dans k (puisqu'il n'y a plus de degrés locaux impairs), ce qui est le cas, en vertu de l'égalité $(\lambda_1 + \lambda_1^{-1})(a) = \sqrt{2}$, si $\lambda_1 + \lambda_1^{-1}$ est défini sur k, c'est-à-dire si l'on a $s \geqslant 1$. Finalement cette condition globale n'existe que pour $s = 0$, $r = 3$. Pour les conditions locales (qui n'existent que pour $r \leqslant 2$), cf. [4]. On retrouve ainsi les conditions de Damey et Martinet ([2], [3]).

BIBLIOGRAPHIE

[1] E. ARTIN, J. TATE, Class field theory, Benjamin,1968.

[2] P. DAMEY, Sur certaines 2-extensions galoisiennes non abéliennes d'un corps de caractéristique différente de deux, Thèse (Grenoble), 1971.

[3] P. DAMEY, J. MARTINET, Plongement d'une extension quadratique dans une extension quaternionienne, *J. reine angew. Math.*, 262-263 (1973), 323-338.

[4] R. GILLARD, Sur le problème du plongement des extensions galoisiennes, Thèse de troisième cycle (Grenoble),1973.

[5] H. HASSE, Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers, *Math. Nachr.*, 1 (1948), I 40-61, II 213-217, III 277-283.

[6] K. HOECHSMANN, Zum Einbettungsproblem, *J. Reine angew. Math.*, 229 (1968), 81-106.

[7] M. IKEDA, Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem, *Hamb. Abh.*, 24 (1960), 126-131.

[8] J. NEUKIRCH, Über das Einbettungsproblem der algebraischen Zahlentheorie, *Inventiones math.*, 21 (1973), 59-116.

[9] J.-P. SERRE, Cohomologie galoisienne, *Springer Lecture Notes*, 5 (1964).

[10] J. TATE, Duality Theorems in Galois Cohomology over Number Fields, *Proc. Cong. Stockholm*, (1962), 288-295.

[11] K. UCHIDA, On Tate's Duality Theorems in Galois Cohomology, *Tôhoku Math. J.*, 21 (1969), 92-101.

Manuscrit reçu le 28 février 1977.

Georges POITOU,
Université de Paris-Sud
Centre Scientifique d'Orsay
Mathématiques
Bâtiment 425
91405 Orsay Cedex.