ANNALES DE L'INSTITUT FOURIER

BERNADETTE PERRIN-RIOU

Plongement d'une extension diédrale dans une extension diédrale ou quaternionienne

Annales de l'institut Fourier, tome 30, n° 4 (1980), p. 19-33

<http://www.numdam.org/item?id=AIF_1980__30_4_19_0>

Ann. Inst. Fourier, Grenoble
30, 4 (1980), 19-33.

PLONGEMENT D'UNE EXTENSION DIÉDRALE DANS UNE EXTENSION DIÉDRALE OU QUATERNIONIENNE

par Bernadette PERRIN-RIOU

Soit K/k une extension galoisienne de groupe de Galois G et E un groupe dont G est un quotient ; on se demande s'il existe une surextension N/k contenant K, de groupe de Galois isomorphe à E et telle que la restriction des automorphismes corresponde au passage au quotient $E \to G$. Une telle extension N est dite solution du problème de plongement relatif à E et à K/k.

Ces problèmes de plongement ont été principalement étudiés dans le cas où les groupes E et G sont finis et où le noyau A de l'application $E \to G$ est abélien, ce que nous supposerons désormais. Par exemple, ont été considérés surtout pour les corps de nombres, le plongement d'une extension cyclique dans une extension cyclique de degré supérieur [5], [12], le plongement d'une extension quadratique dans une extension diédrale ou quaternionienne [1], [2], [5], [7], [12], le plongement d'une extension abélienne de groupe de Galois de type (p, p) dans une extension de degré p^3 [6], le plongement d'une extension diédrale d'ordre 2^{h+1} dans une extension diédrale ou quaternionienne d'ordre 2^{r+h+1}. Ce dernier problème a été étudié par Witt [15] et par Damey et Payan [3] dans le cas où $h = r = 1$, et pour h et r quelconques par Halter-Koch, dont la méthode paraît limitée au cas où le corps de base est le corps des rationnels [7].

Le présent travail se situe dans la ligne de l'idée de Hasse, consistant à représenter le noyau du plongement par un groupe de nombres, au moyen de caractères. Après la transcription cohomologique de Hœschsmann, Neukirch a observé que la méthode des caractères conduit à des conditions nécessaires et suffisantes dans le cas local et il a donné des conditions pour qu'un problème de plongement se ramène à ses images locales [10]. Poitou a alors

étudié les conditions supplémentaires, dites globales [12]. Nous allons maintenant faire un court rappel de cette méthode, que nous appliquerons ensuite au plongement d'un groupe diédral dans un groupe diédral ou quaternionien.

Le groupe E, extension du groupe G par le sous-groupe A, peut être décrit à isomorphisme près par l'action de G sur A et par un élément ε du groupe de cohomologie $H^2(G,A)$. Soit $\bar{k}$ une clôture algébrique de k et $\bar{G}$ le groupe de Galois de $\bar{k}/k$. Les théorèmes suivants ramènent le problème de plongement à la nullité d'un cocycle de $H^2(\bar{G},A)$.

THÉORÈME (Hœchsmann [8]). — *Une condition nécessaire à l'existence d'une solution est que l'image de* ε *par inflation dans le groupe* $H^2(\bar{G},A)$ *soit nulle.*

Si E est un p-groupe (p étant un nombre premier), on appelle rang de E la dimension sur $\mathbf{Z}/p\mathbf{Z}$ de $H^1(E,\mathbf{Z}/p\mathbf{Z})$.

THÉORÈME (Ikeda [9]), — *Si* E *et* G *sont deux p-groupes de même rang ou si* k *est un corps de nombres, la condition du théorème de Hœchsmann est une condition suffisante.*

Cette condition peut être transcrite grâce aux théorèmes de dualité de Tate-Poitou. Dans le cas local (Neukirch [8]), il faut et il suffit que s'annulent dans $H^2(G,K^X)$ toutes les images $\chi^*(\varepsilon)$ où χ est un caractère de A dans $\bar{k}^X$, défini sur k, c'est-à-dire invariant par $\bar{G}$. Dans le cas global (Poitou [12]), il faut et il suffit que s'annulent dans $H^2(G,\mathscr{C}(K))$ toutes les images $\chi^*(\varepsilon)$ où χ est un caractère, défini sur k, de A dans le groupe $\mathscr{C}$ des classes d'idèles de $\bar{k}$. D'autre part, si on choisit un prolongement de toute place v de k jusqu'à $\bar{k}$ et si on appelle G_v et $\bar{G}_v$ les sous-groupes de décomposition relatifs à v, on appelle condition locale en v la condition d'annulation de l'image de ε par restriction puis inflation dans $H^2(\bar{G}_v,A)$:

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

ce qui est équivalent à la condition d'annulation de tous les $\chi_v^*(\text{res}\,\varepsilon)$ où χ_v décrit les caractères de A dans $\bar{k}_v^X$ définis sur k_v. Ces conditions locales sont équivalentes à la condition d'annulation de $\chi^*(\varepsilon)$ pour tout élément de $\text{Hom}_k(A,\mathscr{C})$ appartenant à l'image de π^* :

$$\text{Hom}_k(A,\mathscr{I}) \xrightarrow{\pi^*} \text{Hom}_k(A,\mathscr{C})$$

($\mathscr{I}$ désigne le groupe des idèles de $\bar{k}$). Si on suppose les conditions locales vérifiées, il suffit d'écrire l'annulation de $\chi^*(\varepsilon)$ pour tout χ représentant les élément du conoyau de π^*. On montre que ce conoyau est fini. Dans le cas où A est cyclique, Poitou a montré qu'il contient un ou deux éléments : il est d'ordre 1 si et seulement si le groupe de Galois de $k(A')/k$ ($A' = \mathrm{Hom}(A, \bar{k}^X)$) est égal à l'un de ses sous-groupes de décomposition ; dans le cas contraire, c'est-à-dire si le groupe de Galois de $k(A')/k$ est non cyclique et distinct de tous ses sous-groupes de décomposition, le conoyau de π^* est d'ordre 2 ; on peut écrire l'élément non nul par ses composantes locales dans $k(A')$.

Dans cet article, on étudie le problème de plongement d'une extension diédrale K/k de degré 2^{h+1} dans une extension diédrale ou quaternionienne N/k de degré 2^{r+h+1} sur une extension p-adique ou sur un corps de nombres quelconques. On parlera en abrégé du problème de plongement diédral ou quaternionien en degré 2^r. Le noyau du plongement est alors cyclique.

1. Généralités sur les groupes diédraux et quaternioniens.

Soit E un groupe diédral ou quaternionien d'ordre 2^{r+h+1} de générateurs σ et τ vérifiant

$$2^{r+h} = 1, \quad \tau^2 = \begin{cases} 1 & \text{(cas diédral)} \\ 2^{r+h-1} & \text{(cas quaternionien)} \end{cases}$$

et

$$\tau\sigma\tau^{-1} = \sigma^{-1}.$$

Soient A le sous-groupe cyclique d'ordre 2^r de E engendré par

$$a = \sigma^{2^h}$$

et G le quotient de E par A ; c'est un groupe diédral engendré par l'image x de σ et l'image y de τ par l'application quotient :

$$x^{2^h} = 1, \quad y^2 = 1, \quad yxy^{-1} = x^{-1}.$$

Ces notations seront conservées tout au long du texte. On notera aussi H le sous-groupe de G engendré par x.

PROPOSITION 1. — *Avec les notations précédentes, le groupe* E *est extension du groupe* G *par le groupe* A. *L'action de* G *sur* A *est déterminée par* $a^x = a$, $a^y = a^{-1}$. *Le cocycle* ε *de l'extension, calculé en utilisant comme*

relèvement de $y^\ell x^j$ *pour* $\ell = 0,1$ *et* $j = 0, \ldots, 2^h - 1$, *l'élément* $\tau^\ell \sigma^j$ *de* E *est alors donné par*

$$\begin{aligned} \varepsilon(x^i,x^j) &= a^{\eta'} \\ \varepsilon(x^i,yx^j) &= a^{-\eta} \\ \varepsilon(yx^i,x^j) &= a^{-\eta'} \\ \varepsilon(yx^i,yx^j) &= a^{\eta+\omega 2^r-1} \end{aligned} \qquad \text{pour} \quad 0 \leqslant i < 2^h, 0 \leqslant j < 2^h$$

où η *est égal à* 0 *si on a* $j - i \geqslant 0$ *et à* -1 *si on a* $j - i < 0$, *où* η' *est égal à* 0 *si on a* $i + j < 2^h$ *et à* 1 *si on a* $i + j \geqslant 2^h$ *et où* ω *est égal à* 0 *dans le cas diédral et à* 1 *dans le cas quaternionien.*

Réciproquement, toute extension d'un groupe diédral G *d'ordre* 2^{h+1} *par un groupe cyclique* A *d'ordre* 2^r *définie à l'aide de cette action et de ce cocycle est isomorphe à un groupe diédral si* ω *est égal à* 0 *et quaternionien si* ω *est égal à* 1, *d'ordre* 2^{r+h+1}.

Soit ψ un homomorphisme de A dans un G-module B tel que $H^1(H,B)$ soit nul (on pourra prendre B égal à K^X si K est un corps p-adique ou $\mathscr{C}(K)$ si K est un corps de nombres). Le dévissage du groupe diédral G en deux groupes cycliques et la suite exacte

$$O \to H^2(G/H,B^H) \xrightarrow{\text{inf}} H^2(G,B) \xrightarrow{\text{res}} H^2(H,B)$$

permet d'écrire la condition nécessaire et suffisante pour que $\psi^*(\varepsilon)$ soit un cobord.

LEMME 2 [11]. — *Posons* $\alpha = \psi^*(\varepsilon)(x,x^{-1})$.

1) *Si* res $\psi^*(\varepsilon)$ *est un cobord, alors* α *est une norme relativement au sous-groupe* H. *Il existe alors des éléments* b *et* c *de* B *vérifiant*

$$N_H(b) = \alpha, \quad c^x c^{-1} = b^{-1} b^{-xy},$$

2) *le cocycle* $\psi^*(\varepsilon)$ *est un cobord si et seulement si* α *est une norme pour* H *et si* $\psi^*(\varepsilon)(y,y)c^{-1}c^{-y}$ *(qui est un élément de* B^H*) est une norme pour* G/H.

2. Traduction de la condition cohomologique.

Dans ce paragraphe, nous allons étudier les conditions de plongement dans un cadre général comprenant à la fois le cas où k est un corps p-adique et le cas où k est un corps de nombres.

Soit K/k une extension galoisienne de groupe de Galois diédral G d'ordre 2^{h+1}. Soit k_0 le sous-corps de K laissé fixe par x. Soit χ le caractère défini de la manière suivante : si k est un corps p-adique, c'est un générateur du sous-groupe des caractères de A dans $\bar{k}^{\times}$ définis sur k ; si k est un corps de nombres, c'est un caractère de A dans $\mathscr{C}$ défini sur k et n'appartenant pas à l'image de π^*. On note C(K) le groupe multiplicatif de K si K est un corps p-adique et le groupe des classes d'idèles de K si K est un corps de nombres. Dans le cas global, on suppose de plus que les conditions locales sont vérifiées. Comme l'on peut appliquer le théorème d'Ikeda déjà cité, la condition de résolubilité du problème de plongement de l'extension K/k dans une extension diédrale ou quaternionienne est que le cocycle $\chi^*(\varepsilon)$ de $H^2(G,C(K))$ est un cobord et c'est ce que l'on va expliciter. Posons $X = \chi^*(\varepsilon)(x,x^{-1})$ et $Y = \chi^*(\varepsilon)(y,y)$. On vérifie facilement que X appartient à $C(k_0)$, que Y et $X^{2^{r-1}}$ appartiennent à $C(k)$ (on a d'ailleurs $Y = X^{2^{r-1}}$ dans le cas quaternionien et $Y = 1$ dans le cas diédral) et que $X^y = X^{-1}$. Il existe donc un élément Z de $C(k_0)$ vérifiant $Z^yZ^{-1} = X$.

On aura besoin du lemme suivant :

LEMME 3. — *Soit* N *une extension diédrale ou quaternionienne sur* k, *cyclique sur* k_0. *Si* z *est un élément de* $C(k)$, *le symbole d'Artin de* z *relatif à l'extension* N/k_0 *est d'ordre* 1 *si* N/k *est diédrale et d'ordre* 1 *ou* 2 *si* N/k *est quaternionienne. Dans ce dernier cas, on a* $(z,N/k_0) = 1$ *si et seulement si* $(z,N/k)$ *appartient à l'image de* $G(N/k_0)$ *dans* $G(N/k)/G(N/k)'$ (*où* $G(N/k)'$ *désigne le groupe des commutateurs de* $G(N/k)$).

Pour la démonstration, on utilise l'application transfert Ver de $G(N/k)$ dans $G(N/k_0)$ que l'on peut calculer ici explicitement et la propriété du symbole d'Artin

$$\text{Ver}\,(z,N/k) = (z,N/k_0).$$

Supposons maintenant qu'il existe une extension N diédrale sur k, cyclique sur k_0 et contenant K, de degré 2^{r+h+1}. Comme $X^{2^{r-1}}$ est un élément de $C(k)$, on a d'après le lemme 3,

$$(X,N/k_0)^{2^{r-1}} = 1.$$

On a de plus les égalités suivantes

$$\begin{aligned}(X,N/k_0) &= (Z/Z^y,N/k_0) = (Z,N/k_0).(y(Z,N/k_0)y^{-1})^{-1}\\ &= (Z,N/k_0)^2.\end{aligned}$$

On en déduit que le symbole d'Artin $(Z,N/k_0)$ est d'ordre divisant 2^r. Son image par l'application quotient $G(N/k_0) \to H$ qui envoie σ sur x est donc égale à 1. Elle est d'autre part égale à l'élément $(Z,K/k_0)$. Donc, Z est la norme d'un élément de C(K).

Supposons maintenant qu'il existe une extension N quaternionienne sur k, cyclique sur k_0, contenant K, de degré 2^{r+h+1}. On a alors

$$X^{2^{r-1}} = Y.$$

Or on vérifie facilement que $(Y,N/k_0)$ est égal à 1 si et seulement si $(Y,k_0/k)$ est égal à 1. Donc, si $(Y,k_0/k)$ est égal à 1, on a

$$(X,N/k_0)^{2^{r-1}} = 1,$$

et on peut conclure comme dans le cas diédral que Z est la norme d'un élément de C(K). Si par contre $(Y,k_0/k)$ est égal à -1, alors d'après le lemme 3, on a

$$(X,N/k_0) = \sigma^{2^{r+h-1}}$$

d'où

$$(Z,N/k_0)^{2^r} = \sigma^{2^{r+h-1}}.$$

Cela implique que $(Z,K/k_0)$ est égal à $x^{2^{h-1}}$ donc d'ordre 2.

On a ainsi trouvé des conditions nécessaires à la résolubilité de ces problèmes de plongement. Ces conditions sont en fait suffisantes.

THÉORÈME 4. — 1) *Le problème de plongement relatif au groupe diédral a une solution si et seulement si* Z *est une norme d'un élément de* C(K).

2) *Le problème de plongement relatif au groupe quaternionien a une solution si et seulement si les symboles d'Artin* $(Z,K/k_0)$ *et* $(Y,k_0/k)$ *sont de même ordre.*

Démonstration. — Il ne reste plus qu'à montrer la suffisance des conditions. Supposons d'abord que Y est une norme pour l'extension k_0/k (ce qui contient le cas diédral). Montrons que la condition $(Z,K/k_0) = 1$ est suffisante. On utilise le lemme 2. Il existe U appartenant à C(K) tel que l'on ait $Z = N_{K/k_0}(U)$. Donc, on a

$$X = N_{K/k_0}(U^y/U).$$

Donc X est une norme dans K/k_0. Prenons $b = U^y/U$. On cherche ensuite un élément c de C(K) vérifiant

$$c^x/c = (U/U^y)^{-1}(U/U^y)^{-xy} = (U/U^y)^x(U/U^y)^{-1},$$

ce qui peut se résoudre par $c = U/U^y$. On a alors $cc^y = 1$, donc

$$(Yc^{-1}c^{-y}, \quad k_0/k) = 1$$

et c'est ce qu'il fallait montrer. La condition $(Z,K/k_0) = 1$ est bien suffisante.

Il reste à étudier le cas où E est quaternionien et où Y n'est pas une norme pour l'extension k_0/k. On remarque que X et donc Z sont définis de la même manière dans le cas diédral et quaternionien. La condition $(Z,K/k_0)$ d'ordre 2 implique que X est norme d'un élément de C(K). Mais dans ce cas, on remarque que le problème diédral est résoluble si et seulement si le problème quaternionien ne l'est pas (voir le lemme 2). Donc si $(Z,K/k_0)$ est d'ordre 2, le problème quaternionien est résoluble, ce qui termine la démonstration.

3. Plongement d'une extension de corps p-adiques.

Le calcul du caractère χ qui intervient dans le théorème 4 est alors facile. On a un isomorphisme entre le groupe des caractères de A dans $\bar{k}^x$ définis sur k et le sous-groupe des racines de l'unité d'ordre divisant 2^r de k_0 et de norme 1 sur k. On note 2^q l'ordre de ce sous-groupe et ζ un générateur. Soit m un élément de k tel que $k_0 = k(\sqrt{m})$. On transcrit le thèorème 4.

THÉORÈME 5. — *En utilisant les notations précédentes, on pose*

$$z = \begin{cases} 1 + \zeta & \text{si} \quad q > 1 \\ \sqrt{m} & \text{si} \quad q = 1 \end{cases}$$

C'est un élément de k_0 dont le quotient par son conjugué sur k est égal à ζ.

La condition pour que le problème de plongement soit résoluble est que $(z,K/k_0)$ soit égal à 1 dans le cas diédral et de même ordre que $(\zeta^{2^{r-1}},k_0/k)$ dans le cas quaternionien.

Pour la démonstration, on applique le théorème 4 : on a alors $X = \zeta$, $Z = z$ et $Y = \zeta^{2^{r-1}}$.

Dans le cas où k est une extension p-adique avec p impair, on peut donner des conditions plus faciles à vérifier.

THÉORÈME 6. — *On suppose que k est une extension p-adique avec p impair. Si l'un des entiers r ou h est strictement supérieur à 1, le problème de plongement aussi bien dans le cas diédral que dans le cas quaternionien admet une solution si et seulement si k ne contient pas les racines de l'unité d'ordre 4, et si k_0 contient les racines de l'unité d'ordre 2^{r+h+1}. Si r et h sont égaux à 1, le problème diédral (resp. quaternionien) admet une solution si et seulement si les racines de l'unité d'ordre 4 n'appartiennent pas à k mais à k_0 (resp. n'appartiennent pas à k).*

Pour montrer que ces conditions sont nécessaires, on utilise les propriétés de ramification modérée. Pour la suffisance, on utilise le théorème 4 et un autre choix de l'élément Z (pour plus de détails, voir [11]).

4. Plongement d'une extension de corps de nombres.

Nous n'étudierons pas ici en détail les conditions locales, qui se ramènent soit au cas étudié dans le paragraphe 3, soit à des situations déjà connues ([5] ; on trouvera tous les détails dans [11]). Aussi s'attachera-t-on à l'étude de la condition globale éventuelle. Or, on a vu que l'existence d'une telle condition est liée à une certaine extension $k(A')$ de k que l'on va calculer.

L'extension $k(A')$ est contenue dans $K(\mu_{2^r})$ où μ_{2^r} est le groupe des racines de l'unité d'ordre divisant 2^r. Mais comme le groupe de Galois de K/k_0 opère trivialement sur A', $k(A')$ est contenue dans $k_0(\mu_{2^r})$. On montre facilement le lemme suivant.

LEMME 7. — *Soit m un élément de k tel que $k_0 = k(\sqrt{m})$. Si $r = 1$, $k(A')$ est égal à k. Si $r \geqslant 2$, $k(A')$ est égal à $k\left(\sqrt{-m}, \cos\dfrac{2\pi}{2^r}\right)$.*

L'étude du groupe de Galois de $k(A')/k$ permet alors d'énoncer [11], [12], m étant toujours un élément de k tel que $k_0 = k(\sqrt{m})$:

THÉORÈME 8. — *Pour que le problème de plongement requière une condition globale, il faut et il suffit que l'on ait les deux conditions suivantes :*

1) *Il existe un entier* s, *compris entre* 0 *et* $r-3$, *tel que, si* ζ *est une racine de l'unité d'ordre* 2^{s+3}, $\zeta^2+\zeta^{-2}$ *appartienne à* k, *mais non* $\zeta+\zeta^{-1}$ *et que le sous-corps* $k(\sqrt{-m},\zeta+\zeta^{-1})$ *de* $k(A')$ *soit biquadratique.*

2) *Toute place de* k *se décompose dans au moins l'une des extensions quadratiques*

$$k(\zeta+\zeta^{-1}),\quad k(\sqrt{-m})\quad\text{et}\quad k((\zeta-\zeta^{-1})\sqrt{m}).$$

On posera alors

$$k'=k(\sqrt{-m}),\quad k(+)=k(\zeta+\zeta^{-1}),\quad k(-)=k((\zeta-\zeta^{-1})\sqrt{m}).$$

On suppose désormais que le problème de plongement requiert une condition globale. Il reste à écrire celle-ci.

L'homomorphisme $\bar{\psi}$ de A dans $\mathscr{C}(k_0)$ qui appartient au conoyau de π^* est décrit entièrement dans [12]. L'image par $\bar{\psi}$ du générateur privilégié de A qu'est $\varepsilon(x,x^{-1})$ est déterminée par l'idèle $\mathscr{J}$ de k' de la manière suivante : la composante de $\mathscr{J}$ en une place de k se décomposant dans k' est $(\zeta^2,1)$ (on note cet ensemble de place I, [12]); la composante de $\mathscr{J}$ en une place v de k ne se décomposant pas dans k' mais dans $k(+)$ est ζ ($v\in$ IIa); la composante de $\mathscr{J}$ en une place de k ne se décomposant pas dans k' mais dans $k(-)$ est $i\zeta$ ($v\in$ IIb); ce que l'on peut noter :

$$\mathscr{J}=((\zeta^2,1)_{v\in \mathrm{I}},\quad(\zeta)_{v\in \mathrm{II}a},\quad(i\zeta)_{v\in \mathrm{II}b}).$$

Soit X la classe d'idèles de $\mathscr{C}(k_0)$ égale à $\bar{\psi}(\varepsilon(x,x^{-1}))$.

On cherche un représentant de X appartenant à $\mathscr{J}(k_0)$. Pour cela, il suffit de trouver un élément u de k_0k' tel que $u^{-1}\zeta$ appartienne à $k_0k(+)$ et tel que $u^{-1}(i\zeta)$ appartienne à $k_0k(-)$. Dans le cas particulier où k' est égal à k_0, $\mathscr{J}$ est déjà un élément de $\mathscr{J}(k_0)$; sinon, on peut choisir $u=1+\zeta^2$. La norme de l'idèle $u^{-1}\mathscr{J}$ de $\mathscr{J}(k_0)$ est un élément de k^X; c'est exactement

$$\frac{\zeta^2}{(1+\zeta^2)^2}$$

(ζ^2 dans le cas où k' est égal à k_0). D'autre part, il existe un élément a de k_0 dont la norme est égale à la norme de $u^{-1}\mathscr{J}$:

$$N_{k_0/k}(a) = \frac{\zeta^2}{(1+\zeta^2)^2} \quad (\text{ou } \zeta^2)$$

et un idèle U de k_0 vérifiant $U/U^y = u^{-1}a^{-1}\mathscr{J}$. On note U_w la composante de U relative à la place w de k_0. On a le théorème :

THÉORÈME 9. — *On suppose les conditions locales relatives au problème de plongement vérifiées et on suppose que l'extension $k(A')/k$ a un groupe de Galois non cyclique et distinct de tous ses sous-groupes de décomposition (en particulier $r \geqslant 3$). Le problème de plongement relatif au groupe diédral a une solution si et seulement si on a :*

$$\prod_w (U_w, K/k_0)_w = 1$$

le produit ayant lieu sur les places w de k_0. La condition de résolubilité du plongement relatif au groupe quaternionien est :

1) *si s est strictement inférieur à $r-3$ ou si $\prod_{v\in I}(-1,k_0/k)_v$ est égal à 1,*

$$\prod_w (U_w, K/k_0)_w = 1$$

2) *sinon :*

$$\prod_w (U_w, K/k_0)_w \quad \text{d'ordre 2.}$$

Démonstration. — Ceci est la transcription du théorème 4, si on remarque que $Y = \bar{\psi}(\varepsilon(y,y))$ est égal à la classe d'idèles de $((1)_{v\in I}, (-1)_{v\in II})$ dans le cas quaternionien, $r = s+3$, et à 1 sinon.

On a en effet $X^{2^{s-1}} = ((1)_{v\in I}, (-1)_{v\in II})$. L'élément Z du théorème 4 est ici appelé U.

Remarque. — Les seules places $w|v$ pouvant apporter une contribution différente de 1 à $\prod_w (U_w, K/k_0)_w$ sont, outre celles divisant 2, les places se ramifiant dans K/k_0 et les places divisant l'élément a de norme $\zeta^2/(1+\zeta^2)^2$.

Quant au calcul de U, il se fait place par place lorsqu'on a trouvé l'élément a. On peut donc effectivement calculer les conditions de plongement. Dans le paragraphe suivant, nous allons réécrire le théorème 8 dans quelques cas particuliers.

5. Exemples.

PROPOSITION 10. — *On suppose que* $K/\mathbf{Q}$ *est une extension diédrale cyclique sur* $k_0 = \mathbf{Q}(\sqrt{m})$, *où* m *est un entier de* $\mathbf{Q}$ *sans facteurs carrés. Alors, le problème de plongement requiert une condition globale si et seulement si* r *est supérieur à* 3, *si* m *est différent de* -1 *et de* -2, *s'il est congru à* -1 *ou à* -2 *modulo* 8, *si* 2 *est une norme dans l'extension* $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$.

Dans le cas contraire, le problème de plongement a une solution si et seulement si les conditions locales sont vérifiées.

Ici, l'élément a du théorème 9 est égal à 2.

Des calculs de condition globale sont faits dans [11]. Remarquons d'autre part que le théorème 9 permet des comparaisons simples entre les problèmes diédraux et quaternioniens. Par exemple, la condition globale peut être vérifiée dans le cas quaternionien pour r égal à 3 et ne l'être jamais dans le cas diédral, par exemple $K = \mathbf{Q}(\sqrt{7},\sqrt{113})$, $k_0 = \mathbf{Q}(\sqrt{7})$, ou l'être dans le cas diédral pour r supérieur à 3 et dans le cas quaternionien pour r strictement supérieur à 3, par exemple $K = \mathbf{Q}(\sqrt{7},\sqrt{127})$, $k_0 = \mathbf{Q}(\sqrt{7})$.

Donnons maintenant quelques exemples où le corps de base est différent du corps des rationnels.

PROPOSITION 11. — *On suppose que* $K/\mathbf{Q}(i)$ *est une extension diédrale cyclique sur* $k_0 = \mathbf{Q}(i,\sqrt{m})$ *où* m *est un entier de* $\mathbf{Q}(i)$ *sans facteurs carrés; alors le problème de plongement admet une condition globale si et seulement si* r *est supérieur à* 3, *si* m *est différent de* ± 2, *si* m *ou* $2m$ *est un carré dans* $\mathbf{Q}_2(i)$ *et si* 2 *est une norme dans l'extension* $\mathbf{Q}(i,\sqrt{m})/\mathbf{Q}(i)$. *Dans le cas contraire, le problème de plongement a une solution si et seulement si les conditions locales sont vérifiées.*

Soit ζ *une racine de l'unité d'ordre* 2^h *et* K *une extension diédrale de* $\mathbf{Q}(\zeta+\zeta^{-1})$, *cyclique sur* $\mathbf{Q}(\zeta)$, *de degré* 2^{h+1}. *Alors, cette extension se plonge dans une extension diédrale si et seulement si les conditions locales sont vérifiées.*

Remarquons que, de façon générale, si S est un ensemble de places de k, il est intéressant de savoir s'il existe une solution N au problème de plongement telle que l'extension N/k soit non ramifiée au dehors de S. Un tel problème se traite de manière identique [11], en utilisant les théorèmes de dualité à ramification limitée de Tate [13], (voir aussi [14]). Par exemple, si $K/\mathbf{Q}(\zeta+\zeta^{-1})$ est une extension diédrale cyclique sur $\mathbf{Q}(\zeta)$ (voir dernier exemple), si S est un ensemble de places de $\mathbf{Q}(\zeta+\zeta^{-1})$ contenant les places se ramifiant dans K et si $K/\mathbf{Q}(\zeta+\zeta^{-1})$ se plonge dans une extension diédrale (cyclique sur $\mathbf{Q}(\zeta)$), elle se plonge dans une extension diédrale non ramifiée au dehors de S. Cela se déduit facilement, à partir de la théorie générale, du fait que le nombre de classes de $\mathbf{Q}(\zeta+\zeta^{-1})$ est impair (Weber). On peut aussi démontrer une généralisation d'un théorème de Fröhlich [4].

THÉORÈME 12 [11]. — *Soit* $K/\mathbf{Q}$ *une extension diédrale de degré* 2^{h+1}. *Soit* S *un ensemble de places de* $\mathbf{Q}$ *contenant la place infinie et les places se ramifiant dans* $K/\mathbf{Q}$. *On suppose de plus que l'une des trois conditions suivantes est vérifiée :*

(i) 2 *appartient à* S

(ii) *il existe un nombre premier* p *de* S *non congru à* ∓ 1 *modulo* 8

(iii) *le groupe de décomposition en* 2 *de* $G(K/\mathbf{Q})$ *est nul.*

Alors si l'extension $K/\mathbf{Q}$ *est plongeable dans une extension diédrale* (resp. *quaternionienne*) *de degré* 2^{h+2}, *alors elle est plongeable dans une extension diédrale* (resp. *quaternionienne*) *de degré* 2^{h+2} *non ramifiée au dehors de* S.

Tables.

Le tableau donne la liste pour d croissant des corps $\mathbf{Q}(\sqrt{m},\sqrt{d})$ plongeables dans une extension diédrale ou quaternionienne sur $\mathbf{Q}$, de degré 2^{r+2} avec r supérieur à 3, cyclique sur $\mathbf{Q}(\sqrt{m})$. En fait, les listes sont complètes jusqu'à $d = 400$; au delà, figurent seulement les nombres d dont les facteurs premiers sont inférieurs à 400. Pour chaque corps figure en dernière colonne la valeur du produit $\prod_w (U_w \mathbf{Q}(\sqrt{m},\sqrt{d})/\mathbf{Q}(\sqrt{m}))_w$ calculé à l'aide de l'élément de norme 2 indiqué (voir théorème 9). Les colonnes $\mathscr{H}$ et $\mathscr{D}$ donnent la liste de valeurs de r pour lesquels le problème de plongement dans une extension quaternionienne ($\mathscr{H}$) ou diédrale ($\mathscr{D}$) de degré 2^{r+2} sur $\mathbf{Q}$, cyclique sur $\mathbf{Q}(\sqrt{m})$ est possible.

$m = 7 \qquad N(3+\sqrt{7}) = 2$

TABLEAU

	$\mathscr{H}$ $r =$	$\mathscr{D}$ $r =$	
$\mathbf{Q}(\sqrt{7}, \sqrt{79})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{113})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{127})$	4, 5, 6	1, 2, 3, 4, 5, 6	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{158})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{191})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{193})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{226})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{239})$	/	1, 2, 3	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{254})$	4, 5, 6	1, 2, 3, 4, 5, 6	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{337})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{382})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{386})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{478})$	/	1, 2, 3	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{674})$	3	1, 2	− 1
⋮			
$\mathbf{Q}(\sqrt{7}, \sqrt{8\,927})$	/	1, 2, 3	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{10\,033})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{4\,351})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{15\,089})$	/	1, 2, 3	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{15\,247})$	/	1, 2, 3	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{17\,854})$	/	1, 2, 3	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{18\,881})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{20\,066})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{7}, \sqrt{21\,583})$	/	1, 2, 3	+ 1
$\mathbf{Q}(\sqrt{7}, \sqrt{21\,809})$	/	1, 2, 3	+ 1

à partir de $\mathbf{Q}(\sqrt{7}, \sqrt{401})$, la liste n'est plus exhaustive.

$m = 31 \qquad N(39+7\sqrt{31}) = 2$

TABLEAU

	$\mathscr{H}$ $r =$	$\mathscr{D}$ $r =$	
$\mathbf{Q}(\sqrt{31}, \sqrt{47})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{94})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{97})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{113})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{191})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{193})$	4, 5	1, 2, 3, 4, 5	1
$\mathbf{Q}(\sqrt{31}, \sqrt{194})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{226})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{257})$	4, 5, 6, 7	1, 2, 3, 4, 5, 6, 7	1
$\mathbf{Q}(\sqrt{31}, \sqrt{382})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{386})$	4, 5	1, 2, 3, 4, 5	1
$\mathbf{Q}(\sqrt{31}, \sqrt{4\,559})$	/	1, 2, 3	1
$\mathbf{Q}(\sqrt{31}, \sqrt{5\,311})$	/	1, 2, 3	1
$\mathbf{Q}(\sqrt{31}, \sqrt{8\,977})$	/	1, 2, 3	1
$\mathbf{Q}(\sqrt{31}, \sqrt{9\,071})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{10\,961})$	/	1, 2, 3	1
$\mathbf{Q}(\sqrt{31}, \sqrt{12\,079})$	3	1, 2	− 1
$\mathbf{Q}(\sqrt{31}, \sqrt{18\,721})$	3	1, 2	− 1

BIBLIOGRAPHIE

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

[2] P. DAMEY et J. MARTINET, Plongement d'une extension quadratique dans une extension quaternionienne, *J. reine angew. Math.*, 262-263 (1973), 323-338.
[3] P. DAMEY et J.-J. PAYAN, Existence et construction des extensions non abéliennes de degré 8 d'un corps de caractéristique différente de 2, *J. reine angew. Math.*, 244 (1970), 37-82.
[4] A.FRÖHLICH, Artin Root Numbers and Normal Integral Basis, *Inventiones Math.*, 17 (1972), 143-166.
[5] R. GILLARD, Sur le problème du plongement des extensions galoisiennes, Thèse de troisième cycle, Grenoble, 1973.
[6] R. GILLARD, Plongement d'une extension d'ordre p ou p^2 dans une surextension non abélienne d'ordre p^3, *J. reine angew. Math.*, 268-269 (1974), 418-426.
[7] F. HALTER-KOCH, Construction of continuous idele class characters in quadratic number fields and embedding problems for dihedral and quaternion fields, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 17e année (1975/76), n° 14, 13 p.
[8] K. HOECHSMANN, Zum Einbettungsproblem, *J. reine angew. Math.*, 229 (1968), 81-106.
[9] M. IKEDA, Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren, *Abh. Math. Seminar Univ. Hamburg*, 24 (1960), 126-131.
[10] J. NEUKIRCH, Über das Einbettungsproblem der algebraischen Zahlentheorie, *Inventiones Math.*, 21 (1973), 59-116.
[11] B. PERRIN-RIOU, Plongement d'une extension diédrale dans une extension diédrale ou quaternionienne, Thèse de troisième cycle (1979), Publ. math d'Orsay, n° 79-04.
[12] G. POITOU, Conditions globales pour les problèmes de plongement à noyau abélien, *Ann. Inst. Fourier*, 29 (1979), 1-14.
[13] J. TATE, Duality Theorems in Galois Cohomology over Number Fields, Proc. Cong. Stockholm, (1962), 288-295.
[14] K. UCHIDA, On Tate's Duality Theorems in Galois cohomology, *Tôhoku Math. J.*, 21 (1969), 92-101.
[15] E. WITT, Konstruktion von galoisschen Körpern der charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. reine angew. Math.*, 174 (1936), 237-245.

Manuscrit reçu le 14 février 1980.

Bernadette PERRIN-RIOU,
Université Pierre et Marie Curie
Laboratoire de Mathématiques Fondamentales
Aile 45-46, 3e étage
4, place Jussieu
75230 Paris Cedex 05.