MÉMOIRES DE LA S. M. F.

ROLAND GILLARD

Exemples de plongements d'extensions galoisiennes

Mémoires de la S. M. F., tome 37 (1974), p. 87-90

<http://www.numdam.org/item?id=MSMF_1974__37__87_0>

Journées arithmétiques [1973, Grenoble]
Bull. Soc. math. France,
Mémoire 37, 1974, p. 87-90

EXEMPLES DE PLONGEMENTS D'EXTENSIONS GALOISIENNES

par

Roland GILLARD

-:-:-:-

I. INTRODUCTION.

Soit p un nombre premier. Soient E un groupe non abélien d'ordre p^3, A un sous-groupe distingué de E et G le quotient E/A. Soit K/k une extension galoisienne de corps de nombres dont le groupe de Galois est isomorphe à G. On cherche s'il existe une surextension galoisienne N/k de groupe de Galois isomorphe à E telle que le passage au quotient $E \to G$ corresponde sur les groupes de Galois à la restriction des k-automorphismes de N à K. Si une telle surextension existe on dit que le plongement est possible.

Si p est égal à 2, il existe à isomorphisme près deux groupes non abéliens d'ordre 8. Le groupe quaternionien E_1 engendré par deux éléments a et b vérifiant les relations :

$$a^4 = 1 \quad , \quad b^2 = a^2 \quad , \quad bab^{-1} = a^{-1} \quad ;$$

et le groupe diédral E_2 engendré par deux éléments a et b vérifiant :

$$a^4 = 1 \quad , \quad b^2 = 1 \quad , \quad bab^{-1} = a^{-1} \quad .$$

Si p est impair, il existe à isomorphisme près deux groupes non abéliens d ordre p^3 : le groupe E'_1 est engendré par trois éléments vérifiant :

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

et le groupe E'_2 engendré par deux éléments a et b vérifiant :

$$a^{p^2} = b^p = 1 \quad , \quad bab^{-1} = a^{1+p} \quad .$$

Pour chaque place v de k, on choisit un prolongement encore noté v à la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$. On note k_v et K_v les complétés correspondants, on désigne par G_v le groupe de décomposition de v dans K/k. On note ζ_p et ζ_{p^2} des racines primitives de l'unité d'ordre p et p^2. On

appelle k' et K' les corps obtenus par adjonction de ζ_p à k et K.

On étudie le problème de plongement par une méthode qui s'inspire de [3] (pour les détails, voir [4]). Distinguons deux parties suivant l'ordre de G.

II. G D'ORDRE p.

Dans ce § , on suppose que K/k est une extension cyclique de corps de nombres de degré p. On peut distinguer trois cas :

1. E est extension décomposée de A par G (ceci peut arriver pour $p = 2$ et $E = E_2$ ou pour $p \neq 2$ et $E = E'_1$ ou $E = E'_2$). On sait alors que le plongement est toujours possible.

2. Cas où $p = 2$ et $E = E_1$. Posons $K = k(\sqrt{\alpha})$. On peut alors énoncer :
Théorème 1. Si $p = 2$ et $E = E_1$, le plongement est possible si et seulement si toutes les places réelles de k restent réelles dans K, et si pour toutes les places au-dessus de 2 telles que $(-\alpha)$ soit dans $(k_v^*)^2$, le degré local $[k_v : \mathbb{Q}_2]$ est pair.

   On retrouve ainsi le résultat correspondant de [1].

3. Cas où $p = 2$, $E = E_2$, ou $p \neq 2$, $E = E'_2$, A étant engendré par a^p et b. On peut énoncer :
Théorème 2. Dans ce cas le plongement est toujours possible.

   Remarque : Le cas n°3 pour $p \neq 2$ est un exemple de plongement toujours possible bien que E n'y soit pas extension décomposée de A par G.

III. G D'ORDRE p^2.

Dans ce cas A est un sous-groupe distingué d'ordre p de E : c'est donc le centre ; de plus le quotient G est de type (p,p). Dans la suite K/k désigne donc une extension galoisienne de corps de nombres, de type (p,p). La méthode utilisée consiste à se ramener à des conditions "locales" sur K_v/k_v pour chaque place v. On ne sait pas expliciter toutes ces conditions. L'hypothèse restrictive suivante a pour but de tourner la difficulté :

Hypothèse (valable jusqu'à la fin de la conférence) : Il existe une place au plus de k' sauvagement ramifiée et non décomposée dans K'/k'.

Cette hypothèse est vérifiée lorsque k est égal à $\mathbb{Q}$ ou à $\mathbb{Q}(\zeta_p)$. Avec cette hypothèse on peut énoncer :

Théorème 3. Pour $p = 2$ et $E = E_1$, le plongement est possible si et seulement si, pour toute place v décomposée (partiellement ou totalement) dans K/k, -1 est norme de K_v/k_v, et si, pour toute place v non décomposée dans K/k, $\sqrt{-1}$ n'appartient pas à k_v.

Théorème 4. Pour $p = 2$, $E = E_2$ et $K = k(\sqrt{\alpha}, \sqrt{\beta})$, K se plonge dans une surextension diédrale de degré 8 sur k et cyclique sur $k(\sqrt{\alpha})$ si et seulement si β est norme de $k(\sqrt{-\alpha})/k$.

On retrouve le résultat de [2].

Théorème 5. Pour $p \neq 2$ et $E = E'_1$, le plongement est possible si et seulement si toute place de k première à p est décomposée (partiellement ou totalement) dans K.

Théorème 6. Pour $p \neq 2$ et $E = E'_2$, désignons par $\bar{b}$ l'image de b dans G et par H le sous-groupe de G engendré par $\bar{b}$. Pour que le plongement soit possible, il faut et il suffit que les conditions "locales" (cf. ci-dessous) soient vérifiées pour toutes les places v de k :

v	condition locale
$G_v \subset H$	condition vérifiée
G_v d'ordre p et $G_v \neq H$	condition locale vérifiée si et seulement si $\zeta_p \notin k_v$ ou $\zeta_p \in N_{K_v/k_v} K_v$
G_v d'ordre p^2 et $p \nmid v$ ce qui implique : $\zeta_p \in k_v$ et $\zeta_{p^2} \in K_v$	condition locale vérifiée si et seulement si le prolongement de $\bar{b}$ à K_v opère sur ζ_{p^2} par élévation à la puissance $(1+p)$
G_v d'ordre p^2 $p \mid v$ (une place au plus de ce type)	la condition locale est conséquence des conditions précédentes

-:-:-:-

BIBLIOGRAPHIE

[1] P. DAMEY. - Extensions quaternioniennes d'un corps de nombres. Conférence aux Journées arithmétiques de Grenoble (février 1973).

[2] P. DAMEY et J.J. PAYAN. - Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2. J. reine angew. Math. n° 244, (1970) pp. 37-54.

[3] K. HOECHSMANN. - Zum Einbettungsproblem. J. reine angew. Math. n° 229 (1968) pp. 81-106.

[4] R. GILLARD. - Sur le problème du plongement des extensions galoisiennes. Thèse de 3e cycle, Grenoble, 1973.

-:-:-:-

Université de Grenoble I
Institut de Mathématiques Pures
Laboratoire C.N.R.S. associé, n° 188
BP 116
38402-ST MARTIN D'HERES