Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Richard Massy
Thong Nguyen-Quang-Do

# Extensions non abéliennes de degré $p^3$ d'un corps de nombres : étude locale-globale

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 17, n° 1 (1975-1976), exp. n° 19, p. 1-13

<http://www.numdam.org/item?id=SDPP_1975-1976__17_1_A17_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
17e année, 1975/76, n° 19, 13 p.



23 février 1976

# EXTENSIONS NON ABÉLIENNES DE DEGRÉ $p^3$ D'UN CORPS DE NOMBRES : ÉTUDE LOCALE-GLOBALE

par Richard MASSY et Thong NGUYEN-QUANG-DO

## Introduction.

Soient une extension de groupes finis :

$$(\varepsilon) \qquad 1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

de noyau abélien $A$, décrite par une classe de cohomologie $\varepsilon \in H^2(G, A)$, et $K/k$ une extension galoisienne de corps de nombres, dont le groupe de Galois est isomorphe à $G$. Le problème de plongement relatif à $K/k$ et $\varepsilon$ (en abrégé : problème $(K/k, \varepsilon)$) consiste à chercher une surextension $L/k$, galoisienne, de groupe de Galois isomorphe à $E$, et telle que le passage au quotient $E \longrightarrow G$ corresponde sur les groupes de Galois à la restriction des automorphismes de $L$ à $K$. Autrement dit, l'extension des groupes de Galois est décrite par la même classe $\varepsilon$.

Nous nous proposons ici de résoudre le problème de plongement dans le cas où $E$ est un groupe non abélien d'ordre $p^3$ ($p$ étant un nombre premier), et $G$ un quotient de $E$ de type $(p, p)$, en utilisant la théorie de Kummer et des méthodes "globales-locales". Ce problème avait été étudié par R. GILLARD [5], mais résolu seulement de façon partielle.

## 1. Rappels sur le problème de plongement.

On sait, d'après HOECHSMANN [6], que le problème général de plongement $(K/k, \varepsilon)$ admet une solution si, et seulement si, $\inf \varepsilon = 0$, où inf désigne l'inflation : $H^2(G, A) \xrightarrow{\inf} H^2(\overline{G}, A)$, et $\overline{G}$ le groupe de Galois d'une clôture algébrique de $k$ contenant $K$.

Dans le cas particulier où $G$ et $A$ sont des $p$-groupes (on dira alors qu'il s'agit d'un problème de $p$-plongement), on peut prendre pour $\overline{G}$ le groupe de Galois d'une $p$-extension maximale $\overline{k}$ de $k$ contenant $K$. Dans ce cas, soit $k'$ (resp. $K'$) le corps obtenu en ajoutant à $k$ (resp. $K$) les racines $p$-ièmes de l'unité. Le groupe $G' = \mathrm{gal}(K'/k')$ s'identifie canoniquement à $G$ et on a le théorème de réduction suivant.

THÉORÈME 1. - *Pour que le problème de $p$-plongement $(K/k, \varepsilon)$ admette une solution, il faut et il suffit qu'il en soit de même pour le problème $(K'/k', \varepsilon)$.*

*Démonstration.* - Voir par exemple [5], théorème 5.

Considérons maintenant le cas encore plus particulier d'un p-plongement à noyau d'ordre p (i. e. A est supposé cyclique d'ordre p et G opère trivialement sur A ).

Pour toute place v de k , finie ou non, choisissons un plongement de v à $\overline{k}$ , noté aussi v , correspondant à des groupes de décomposition $G_v$ et $\overline{G}_v$ dans G et $\overline{G}$ , et à des complétés $k_v$ et $K_v$ de k et K .

Le diagramme suivant :

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

où les flèches horizontales sont des produits de restrictions et les flèches verticales des inflations, est commutatif. Pour toute place v , soit $\varepsilon_v$ la restriction de $\varepsilon$ dans $H^2(G_v, A)$ . La classe $\varepsilon_v$ est associée à la suite exacte : $1 \longrightarrow A \longrightarrow E_v \longrightarrow G_v \longrightarrow 1$ , où $E_v$ est l'image réciproque de $G_v$ dans E .

D'après [3] (théorème 2, p. 300), la flèche h est injective ; donc $\inf_{G \to \overline{G}} \varepsilon = 0$ si, et seulement si, $\inf_{G_v \to \overline{G}_v} \varepsilon_v = 0$ . Cette deuxième condition sera appelée condition locale en v , associée au problème $(K/k\ ,\ \varepsilon)$ .

On a ainsi montré le "principe local-global" suivant :

THÉORÈME 2. - Pour que le problème de p-plongement $(K/k\ ,\ \varepsilon)$ , à noyau d'ordre p , admette une solution, il faut et il suffit que toutes les conditions locales associées soient vérifiées.

Remarque. - Si $G_v$ et $E_v$ ont même rang (= nombre minimal de générateurs), la condition locale en v est vérifiée si, et seulement si, ([6], 2.3) le problème de plongement local $(K_v/k_v\ ,\ \varepsilon_v)$ admet une solution.

Il reste maintenant à étudier les conditions locales, ce qu'on va faire par la théorie de Kummer puisque, d'après le théorème 1, on peut supposer que k contient le groupe $\mu_p$ des racines p-ièmes de 1 . Si G est d'ordre $p^2$ , de type $(p\ ,\ p)$ , la condition locale en une place décomposée est très simple (voir par exemple [5], 2). On se limitera donc à examiner les places non décomposées, en utilisant la remarque ci-dessus.

## 2. Etude kummérienne du p-plongement à noyau d'ordre p .

Soit p un nombre premier. Dans toute cette section, $\underset{\sim}{K}$ désignera un corps de caractéristique différente de p , contenant le groupe $\mu_p$ des racines p-ièmes de l'unité. Les raisonnements seront facilités par le langage géométrique suivant.

2.1. Langage géométrique. - Désignons par $\Gamma_K$ l'espace vectoriel $K^*/K^{*p}$ sur le corps premier $\underset{\sim}{F}_p$ . Si $\underset{\sim}{L}/K$ est une extension abélienne élémentaire finie de K

(i. e. une extension abélienne finie dont le groupe de Galois est d'exposant $p$), appelons $P(L/K)$ l'ensemble des points de $\Gamma_K$ représentés par des éléments $a \in K^*$ tels que $K(\sqrt[p]{a}) \subset L$. D'après la théorie de Kummer, l'application

$$L \longmapsto P(L/K)$$

induit une bijection $\pi_K$ de l'ensemble des extensions abéliennes élémentaires de degré $p^m$ de $K$ $(m \geqslant 1)$, sur l'ensemble des sous-espaces de dimension $m$ de $\Gamma_K$.

Cas local. - Si $K$ est un corps $\ell$-adique, i. e. une extension de degré $n$ d'un corps $Q_\ell$ de nombres $\ell$-adiques, on sait ([3], p. 137) que $\dim \Gamma_K = \alpha n + 2$, où $\alpha = 1$ ou $0$ suivant que $\ell = p$ ou $\ell \neq p$. De plus, le symbole de puissance $p$-ième (ou symbole de Hilbert) permet de définir une application

$$\langle . , . \rangle : \Gamma_K \times \Gamma_K \longrightarrow F_p ,$$

bilinéaire, antisymétrique, non dégénérée, que nous ferons abondamment intervenir dans la section 3, en utilisant librement les résultats et le vocabulaire du livre d'ARTIN [1]. En particulier, deux éléments $x$ et $y$ de $\Gamma_K$ sont orthogonaux si, et seulement si, $x$ est une norme de $K(\sqrt[p]{y})$ à $K$.

2.2. Prolongement à noyau d'ordre $p$. - Soit $G$ un $p$-groupe d'automorphismes de $K$, dont le corps fixe est $k$ (alors $k$ contient aussi $\mu_p$). Le groupe $G$ opère de façon naturelle sur $\Gamma_K$.

THÉORÈME 3. - *Les extensions galoisiennes de degré $p$ de $K$ qui sont galoisiennes sur $k$, s'identifient par la bijection $\pi_K$ aux droites du $F_p$-sous-espace vectoriel $\Gamma_K^G$ des vecteurs de $\Gamma_K$ laissés fixes par $G$.*

Démonstration. - C'est un exercice facile de théorie de Galois que de montrer qu'une extension galoisienne de degré $p$, $L = K(\sqrt[p]{a})$, $a \in K^*$, est galoisienne sur $k$ si, et seulement si, $a^{-1}.\sigma a \in K^{*p}$ pour tout $\sigma \in G$. La traduction en langage géométrique est immédiate.

Un sous-espace remarquable de $\Gamma_K^G$ est le sous-espace $\eta(\Gamma_k)$, où $\eta = \eta_{K/k}$ est l'homomorphisme de $\Gamma_k$ dans $\Gamma_K$ induit par l'injection canonique de $k^*$ dans $K^*$. Il intervient de la façon suivante.

2.3. Interprétation cohomologique.

THÉORÈME 4. - *On a une suite exacte :*

$$0 \longrightarrow \Gamma_K^G/\eta(\Gamma_k) \simeq H^1(G , K^{*p}) \xrightarrow{\psi} H^2(G , \mu_p) \xrightarrow{\varphi} H^2(G , K^*) .$$

*Les extensions galoisiennes de degré $p$ de $K$ qui sont galoisiennes scindées sur $k$ (i. e. telles que l'extension des groupes de Galois correspondants est scindée) s'identifient par $\pi_K$ aux droites de $\eta(\Gamma_k)$.*

Définition. - Les classes de cocycles de $\operatorname{Ker}\varphi$ seront appelées admissibles pour $K/k$ .

Démonstration. - Considérons les deux suites exactes de G-modules :

$$1 \longrightarrow K^{*p} \longrightarrow K^* \longrightarrow \Gamma_K \longrightarrow 1 \quad \text{et} \quad 1 \longrightarrow \mu_p \longrightarrow K^* \longrightarrow K^{*p} \longrightarrow 1 .$$

Nous en déduisons les suites exactes de cohomologie :

$$1 \longrightarrow k^* \cap K^{*p} \longrightarrow k^* \longrightarrow \Gamma_K^G \longrightarrow H^1(G , K^{*p}) \longrightarrow 1 ,$$

i. e. $H^1(G , K^{*p}) \simeq \Gamma_K^G/\eta(\Gamma_k)$ et

$$1 \longrightarrow H^1(G , K^{*p}) \xrightarrow{\psi} H^2(G , \mu_p) \xrightarrow{\varphi} H^2(G , K^*) \longrightarrow \dots$$

La dernière suite exacte montre que, pour qu'une classe de cocycles $\varepsilon \in H^2(G,\mu_p)$ soit admissible pour $K/k$ , il faut et il suffit que le problème de plongement $(K/k , \varepsilon)$ admette une solution. On peut expliciter $\operatorname{Ker}\varphi = \operatorname{Im}\psi$ .

Soit $a \in K^*$ représentant un élément de $\Gamma_K^G$ . Pour tout $\sigma \in G$ , choisissons $x_\sigma \in K^*$ tel que $a^{-1}.\sigma a = x_\sigma^p$ . L'application de $G \times G$ dans $\mu_p$ , définie par $a(\sigma , \tau) = x_\sigma.\sigma(x_\tau).x_{\sigma\tau}^{-1}$ est un 2-cocycle (vérification facile), dont la classe dans $H^2(G , \mu_p)$ dépend seulement de la classe de $a$ dans $\Gamma_K^G/\eta(\Gamma_k)$ .

2.4. Cas particulier important. - C'est le cas où G est cyclique. Dans ce cas, on peut expliciter les groupes de cohomologie, et la suite exacte du théorème 4 devient

$$1 \longrightarrow \Gamma_K^G/\eta(\Gamma_k) \xrightarrow{\psi} \mu_p \xrightarrow{\varphi} k^*/Nk^* ,$$

où N désigne la norme de K à k .

La description précédente de $\psi$ montre que, pour qu'une extension galoisienne de degré p , $L = K(\sqrt[p]{a})$ , $a \in K^*$ , soit cyclique (resp. galoisienne scindée) sur k , il faut et il suffit que $a^{-1}.\sigma a = x^p$ , $x \in K^*$ avec $Nx \neq 1$ (resp. $Nx = 1$) .

2.5. Cas local. - Si k est une extension de degré $n_0$ d'un corps $\mathbb{Q}_\ell$ de nombres $\ell$-adiques, on peut préciser le théorème 4.

THÉORÈME 5. - $\dim \Gamma_K^G = \alpha n_0 + 2 - \beta + r - d$ , où :

$\alpha = 1$ (resp. 0) si $\ell = p$ (resp. $\ell \neq p$)

$\beta = 1$ (resp. 0) si $\operatorname{Im}\varphi \neq 0$ (resp. $\operatorname{Im}\varphi = 0$)

$d = \dim H^1(G , \mu_p)$ = nombre minimal de générateurs de G

$r = \dim H^2(G , \mu_p)$ = nombre minimal de relations de G (considéré comme pro-p-groupe).

Démonstration. - Par le corps de classes, on sait que $H^2(G , K^*)$ est cyclique. Comme $H^2(G , \mu_p)$ est d'exposant p , $\operatorname{Im}\varphi$ est de dimension au plus égale à 1 . D'autre part, par la théorie de Kummer, $\operatorname{Ker}\eta$ correspond, par la bijection $\pi_k$ ,

à la sous-extension abélienne élémentaire maximale de $K/k$ . La formule du théorème 5 s'obtient immédiatement en prenant la somme alternée des dimensions dans la suite exacte du théorème 4.

En particulier, si $G$ est cyclique, $\dim \Gamma_K^G/\eta(\Gamma_k) = 1$ ou $0$ suivant que $\mu_p \subset Nk^*$ ou non.

## 3. Résultats locaux.

Soit $p$ un nombre premier. Dans toute cette section, $K/k$ désignera une extension galoisienne de corps $\mathfrak{L}$-adiques, contenant le groupe $\mu_p$ des racines $p$-ièmes de l'unité, et dont le groupe de Galois est abélien de type $(p , p)$ . Il correspond à cette extension, par la bijection $\pi_k$ , un plan $P(K/k)$ . On va chercher quelles conditions doit vérifier ce plan pour que $K/k$ se plonge dans une surextension non abélienne de degré $p^3$ .

(Une grande partie des démonstrations, celle qui est d'ordre purement algébrique, reste valable pour un corps $k$ quelconque, de caractéristique $\neq p$ .)

3.1. Rappels sur les groupes d'ordre $p^3$ . - Si $p \neq 2$ , il existe, à isomorphisme près, deux groupes non abéliens d'ordre $p^3$ , engendrés par générateurs et relations de la façon suivante :

Type $E_1$ : $r^p = s^p = t^p = 1$ , $rsr^{-1}s^{-1} = t$ , $rt = tr$ , $st = ts$ .

Les $(p + 1)$ sous-groupes d'ordre $p^2$ sont de type $(p , p)$ .

Type $E_2$ : $s^p = tp^2 = 1$ , $sts^{-1}t^{-1} = t^p$ .

Parmi les $(p + 1)$ sous-groupes d'ordre $p^2$ , un et un seul est de type $(p , p)$. Si $p = 2$ , il existe, à isomorphisme près, deux groupes non abéliens d'ordre $8$ .

Type $E_1'$ (ou diédral) : $s^2 = t^4 = 1$ , $sts^{-1} = t^{-1}$ .

Parmi les trois sous-groupes d'ordre $4$ , un et un seul est cyclique.

Type $E_2'$ (ou quaternionien) : $t^4 = 1$ , $s^2 = t^2$ , $sts^{-1} = t^{-1}$ .

Les trois sous-groupes d'ordre $4$ sont cycliques.

Dans tous les cas ($p = 2$ ou $p \neq 2$) , le seul sous-groupe normal d'ordre $p$ est le centre, confondu avec le groupe de Frattini.

Enfin, un groupe abélien non élémentaire d'ordre $p^3$ sera dit de type $E_0$ . Parmi ses $(p + 1)$ sous-groupes d'ordre $p^2$ , un et un seul est de type $(p , p)$ .

3.2. Comparaison des prolongements ($p \neq 2$) . - Une extension galoisienne $L/k$ dont le groupe de Galois est de type $E_i$ (resp. $E_j'$) sera dite extension de type $E_i$ (resp. $E_j'$) .

THÉORÈME 6.

(i) S'il en existe, les extensions de $k$ contenant $K$ de type $E_1$ (resp. de type $E_0$, non cycliques sur une sous-extension donnée de $K$ de degré $p$) s'identifient par $\pi_K$ aux droites engendrées par les vecteurs d'une certaine classe non triviale du quotient $\Gamma_K^G/\eta(\Gamma_k)$ $(\eta = \eta_{K/k})$.

(ii) S'il en existe, les extensions de type $E_2$ de $k$ contenant $K$ qui sont non cycliques sur une sous-extension $k_0/k$ de $K$ de degré $p$, s'identifient par $\pi_K$ aux droites de $\Gamma_K^G$ engendrées par les vecteurs d'une certaine classe non triviale du quotient $\Gamma_K^G/\eta_0(\Gamma_{k_0}^H)$, où $\eta_0 = \eta_{K/k_0}$ et $H = \mathrm{Gal}(k_0/k)$.

Démonstration. - Soient $\sigma$ et $\tau$ deux générateurs de $G = \mathrm{Gal}(K/k)$, correspondants aux corps fixes $k_0 = k(\sqrt[p]{\alpha})$ et $k_1(\sqrt[p]{\beta})$, $\alpha$ et $\beta \in k^*$. D'après le théorème 4, toute extension $L/K$ de degré $p$ et abélienne de type $(p, p)$ sur $k_0$, est de la forme $L = K(\sqrt[p]{a})$, $a \in k_0^*$. D'après le théorème 3, cette extension est galoisienne sur $k$ si, et seulement si, $a^{-1}.\tau a = x^p$, $x \in K^*$. Comme $a^{-1}.\tau a \in k_0^*$, cette condition équivaut à $a^{-1}.\tau a = \lambda_0^p \beta^i$, $\lambda_0 \in k_0^*$, $i \in \mathbb{F}_p$. On voit facilement que, pour que $L/k$ soit abélienne, il faut et il suffit que $i = 0$. Dans ce cas, l'extension $L/k$ est abélienne non élémentaire si, et seulement si, elle est la composée avec $K$ d'une extension cyclique de degré $p^2$ de $k$, contenant $k_0$. Si $L/k$ est non abélienne, elle est de type $E_1$ (resp. de type $E_2$) si, et seulement si, $N_{K/k_1} x = 1$ (resp. $\neq 1$), d'après 2.4. Le reste de la démonstration s'ensuit aisément.

C. Q. F. D.

3.3. Plans prolongeables $(p \neq 2)$. - Le plan $P(K/k)$ correspondant par $\pi_k$ à l'extension $K/k$ abélienne de type $(p, p)$, est dit prolongeable de type $E_1$ (resp. de type $E_2$ ou $E_0$, au dessus d'une droite $D(k_0/k) \subset P(k/k)$ image par $\pi_k$ d'une extension $k_0/k$ de degré $p$), s'il existe une extension de $k$ de type $E_1$ (resp. de type $E_2$ ou $E_0$, non cyclique sur $k_0$), contenant $K$.

THÉORÈME 7.

(i) Un plan est prolongeable de type $E_0$ au-dessus d'une droite $D(k_0/k)$ si, et seulement si, cette droite est orthogonale à $\mu_p$.

(ii) Les plans prolongeables de type $E_1$ sont les plans dégénérés.

(iii) Les plans prolongeables de type $E_2$ au-dessus d'une droite $D(k_0/k)$ sont les plans hyperboliques (resp. les plans dégénérés) contenant $D(k_0/k)$ si $D(k_0/k)$ n'est pas orthogonale à $\mu_p$ (resp. est orthogonale à $\mu_p$).

Démonstration. - L'assertion (i) résulte immédiatement de la démonstration du théorème 6. Considérons le cas non abélien : une extension $L = K(\sqrt[p]{a})$, $a \in k_0^*$, est galoisienne sur $k$, non abélienne, non cyclique sur $k_0$, si et seulement si

$a^{-1}.\tau a = x^p = \lambda_0^p \beta^i$ , $\lambda_0 \in k_0^*$ , $i \in \underset{\sim}{F}_p^*$ (notations de la démonstration du théorème 7). Cette condition entraîne, en prenant les normes relativement à $\tau$ , que $\beta \in \mu_p . N_{k_0/k} k_0^*$ . L'extension est de type $E_1$ (resp. de type $E_2$) , d'après 2.4, si, et seulement si, $N_{K/k_1} x = 1$ (resp. $\neq 1$) , ce qui équivaut à $\beta \in N_{k_0/k} k_0^*$ (resp. $\exists\, \xi \in \mu_p$ , $\xi \neq 1$ , tel que $\xi^{-1} \beta \in N_{k_0/k} k_0^*$) .

Remarquons que si $\alpha$ n'est pas orthogonal à $\mu_p$ , le quotient $k^*/Nk_0^*$ est représenté par $\mu_p$ .

Réciproquement, soit $\beta = \xi N_{k_0/k} \lambda_0^{-1}$ , $\lambda_0 \in k_0^*$ , $\xi \in \mu_p$ . Alors

$$N_{k_0/k} \beta = N_{k_0/k} \lambda_0^{-p}$$

d'où, d'après le théorème 90 de Hilbert, $\beta.\lambda_0^p = a^{-1}.\tau a$ , $a \in k_0^*$ .

Le théorème en résulte immédiatement.

Remarque. - Tout plan de $\Gamma_k$ contient au moins une droite orthogonale à $\mu_p$ ($p \neq 2$ ou $p = 2$) .

3.2 bis. Comparaison des prolongements ($p = 2$) .

THÉORÈME 8. - S'il en existe, les extensions de $k$ de type $E_0$ (resp. de type $E_1'$ ou $E_2'$) contenant $K$ , non cycliques (resp. cycliques) sur une sous-extension donnée de $K$ de degré 2 , s'identifient par $\pi_K$ aux vecteurs d'une classe non triviale du quotient $\Gamma_K^G/\eta(\Gamma_k)$ .

Démonstration. - Soient $\sigma_1$ , $\sigma_2$ , $\sigma_3 = \sigma_1 \sigma_2$ les éléments non triviaux de $G = \mathrm{Gal}(K/k)$ . Soient $k_i = k(\sqrt{\alpha_i})$ leurs corps fixes respectifs, $\alpha_1$ et $\alpha_2 \in k^*$ , $\alpha_3 = \alpha_1 \alpha_2$ .

Avant d'appliquer le théorème 3, remarquons que pour tout $\sigma \in G$ les applications de $\Gamma_K$ dans $\Gamma_K$ , définies par : $a \longmapsto a^{-1}.\sigma a$ et $a \longmapsto N_\sigma a = a.\sigma a$ , coïncident.

Une extension quadratique $L = K(\sqrt{a})$ , $a \in K^*$ , est donc galoisienne sur $k$ si, et seulement si, $N_\sigma a = x_\sigma^2$ , $x_\sigma \in K^*$ , pour tout $\sigma \in G$ . En tenant compte du fait que, pour $i = 1$ , $2$ , $3$ , $N_{\sigma_i} a \in k_i$ , on peut répéter le raisonnement suivant du théorème 6 et obtenir les critères suivants de prolongement, qu'on énonce sous forme de lemme.

LEMME 1. - Pour que $L = K(\sqrt{a})$ , $a \in K^*$ , soit galoisienne sur $k$ , il faut et il suffit que $N_{\sigma_1} a = \lambda_1^2 \alpha_2^{\rho_1}$ , $N_{\sigma_2} a = \lambda_2^2 \alpha_1^{\rho_2}$ , et $N_{\sigma_3} a = \lambda_3^2 \alpha_1^{\rho_3}$ , où les $\lambda_i$ sont des éléments de $k_i^*$ et les $\rho_i$ des éléments de $F_2$ , pour $i = 1$ , $2$ , $3$ . De plus, l'extension $L/k$ est :

- abélienne élémentaire si, et seulement si, $\rho_i = 0$ , $\forall\, i$ .
- abélienne non élémentaire, non cyclique sur $k_i$ si, et seulement si, $\rho_i = 0$

et $\rho_j = 1$ pour tout $j \neq i$ .

- diédrale, cyclique sur $k_i$ si, et seulement si, $\rho_i = 1$ et $\rho_j = 0$ pour tout $j \neq i$ .

- quaternionienne si, et seulement si, $\rho_i = 1$ pour tout $i$ .

Le théorème s'ensuit sans difficulté.

3.3 bis. Plans prolongeables ($p = 2$) . - Un plan $P(K/k)$ correspondant par $\pi_k$ à une extension $K/k$ abélienne de type (2.2) est dit prolongeable de type $E_2'$ (resp. de type $E_1'$ , au-dessus d'une droite $D(k_i/k) \subset P(K/k)$ ; resp. de type $E_0$ , au-dessus de $D(k_i/k)$) s'il existe une extension de $k$ contenant $K$ , de type $E_2'$ (resp. de type $E_1'$ , cyclique sur $k_i$ ; resp. de type $E_0$ , non cyclique sur $k_i$ .

Comme pour $p \neq 2$ , le plan $P(K/k)$ est prolongeable de type $E_0$ , au-dessus d'une droite $D(k_i/k)$ , si, et seulement si, cette droite est orthogonale à $-1$ . Pour plus de clarté, nous examinerons séparément les cas diédral et quaternionien.

THÉORÈME 9. - Pour qu'un plan $P(K/k)$ soit prolongeable de type $E_1'$ au-dessus de $D(k_i/k) \subset P(K/k)$ , il faut et il suffit que $P(K/k)$ soit engendré par deux droites orthogonales $D(k_j/k)$ , $j \neq i$ .

Les plans prolongeables de type $E_1'$ se divisent en trois classes :

(i) les plans dégénérés orthogonaux à $-1$ : ce sont les plans $P(K/k)$ qui possèdent un prolongement de type $E_1'$ au-dessus de chaque droite $D(k_i/k)$ , $i=1,2,3$, de $P(K/k)$ .

(ii) les plans dégénérés non orthogonaux à $-1$ : ce sont les plans $P(K/k)$ qui possèdent un prolongement de type $E_1'$ au-dessus des droites $D(k_i/k)$ , $i \neq j$ , où $D(k_j/k)$ est la droite de $P(K/k)$ orthogonale à $-1$ .

(iii) les plans non dégénérés non orthogonaux à $-1$ : ce sont les plans $P(K/k)$ qui possèdent un prolongement de type $E_1'$ au-dessus de la droite de $P(K/k)$ qui est orthogonale à $-1$ .

Démonstration. - Soit $\langle . , . \rangle$ la forme bilinéaire introduite en 2.1. Nous adoptons les notations du lemme 1.

(a) Soit $L/k$ une extension diédrale contenant $K$ . Supposons que $L$ est non cyclique sur les extensions $k_1$ et $k_2$ . La même démonstration que celle du théorème 6 montre que $L = K(\sqrt{a})$ , $a \in k_1^*$ vérifiant $a^{-1}.\sigma_2 a = x^2 = \lambda_1^2 \alpha_2$ , avec $\lambda_1 \in k_1^*$ et $N_{K/k_2} x = 1$ , d'où (mêmes calculs que dans le théorème 7), l'on déduit que $\langle \alpha_1 , \alpha_2 \rangle = 0$ . Pour tout plan $P(K/k)$ , montrons la propriété suivante :

$P(K/k)$ est engendré par deux vecteurs orthogonaux équivaut à $P(K/k)$ n'est pas orthogonal à $-1$ , ou $P(K/k)$ est orthogonal à $-1$ et dégénéré.

En effet : si $P(K/k)$ est orthogonal à $-1$ , tous ses vecteurs sont isotropes

et il est dégénéré.

Par contre : si $P(K/k)$ n'est pas orthogonal à $-1$, soit par exemple $\alpha_1$ le seul vecteur non nul du plan qui soit orthogonal à $-1$, alors, si $\langle \alpha_1 , \alpha_2 \rangle = 1$,

$$\langle \alpha_2 , \alpha_1 \alpha_2 \rangle = \langle \alpha_2 , \alpha_1 \rangle + \langle \alpha_2 , \alpha_2 \rangle = 1 + 1 = 0 ,$$

et la propriété est ainsi démontrée.

(b) Réciproquement, soit $P(K/k)$ engendré par deux vecteurs orthogonaux $\alpha_1$ et $\alpha_2$. Alors $\alpha_1 = N_{k_2/k} \lambda_2$, $\lambda_2 \in k_2^*$ d'où, par le même raisonnement que dans le théorème 7, il existe une extension de type $E_1'$, non cyclique sur $k_1$ et $k_2$, donc cyclique sur $k_3$.

(c-i) Si $P(K/k)$ est orthogonal à $-1$ et dégénéré, tous les vecteurs de ce plan sont orthogonaux entre eux, et (b) montre qu'on peut construire, pour tout $1 \leqslant i \leqslant 3$, une extension de type $E_1'$, cyclique sur $k_i$. Réciproquement, si $P(K/k)$ est prolongeable de type $E_1'$ au-dessus de ses trois droites, (a) montre que $\langle \alpha_1 , \alpha_2 \rangle = 0$, $\langle \alpha_2 , \alpha_1 \alpha_2 \rangle = 0$ et $\langle \alpha_1 , \alpha_1 \alpha_2 \rangle = 0$, d'où visiblement $P(K/k)$ est dégénéré et orthogonal à $-1$.

(c-ii) Si $P(K/k)$ est dégénéré, non orthogonal à $-1$, soit $\alpha_1$ le seul vecteur non nul de $P(K/k)$ orthogonal à $-1$. Alors $\alpha_1$ est orthogonal à tout vecteur du plan, donc d'après (b), il existe des prolongements de type $E_1'$ au-dessus de $k_2$ et $k_3$, et d'après (i), il n'en existe pas au-dessus de $k_1$. Réciproquement, si $P(K/k)$ admet des prolongements de type $E_1'$ au-dessus de $k_2$ et $k_3$ et pas au-dessus de $k_1$, $P(K/k)$ n'est pas orthogonal à $-1$, d'après (a) et (c-i). De plus, d'après (a), $\alpha_1$ est orthogonal à $\alpha_2$ et $\alpha_3$. Enfin, d'après le lemme 1, si $K(\sqrt{a_2})$ et $K(\sqrt{a_3})$ sont deux extensions de type $E_1'$ au-dessus de $k_2$ et $k_3$, $K(\sqrt{a_2 a_3})$ est de type $E_0$ au-dessus de $k_1$, donc $\alpha_1$ est orthogonal à $-1$.

(c-iii) Si $P(K/k)$ est non dégénéré, non orthogonal à $-1$, soit $\alpha_1$ le seul vecteur non nul orthogonal à $-1$. Alors $\alpha_1$ ne peut être orthogonal à aucun autre vecteur non nul du plan, sinon celui-ci serait dégénéré. Donc $\langle \alpha_2 , \alpha_3 \rangle = 0$, et d'après (b), il existe un prolongement de type $E_1'$ au-dessus de $k_1$. S'il existait un prolongement de type $E_1'$ au-dessus de $k_2$ par exemple, $\alpha_3$ serait orthogonal à $-1$, d'après la fin de la démonstration de (c-ii) : impossible. Réciproquement, si $P(K/k)$ admet un prolongement de type $E_1'$ au-dessus de $k_1$, mais pas au-dessus de $k_2$ et $k_3$, il résulte de (c-i), et de (c-ii) que $P(K/k)$ est non dégénéré, non orthogonal à $-1$.

C. Q. F. D.

THÉORÈME 10. - Les plans prolongeables de type $E_2'$ sont les plans dégénérés orthogonaux à $-1$ et les plans non dégénérés non orthogonaux à $-1$.

Démonstration. - Montrons d'abord un lemme.

LEMME 2. - Tout plan prolongeable de type $E_2'$ est prolongeable de type $E_1'$.

En effet, si $K(\sqrt{a})$ est de type $E_2'$ et $K(\sqrt{a_1})$ est de type $E_0$ au-dessus de $k_1$, alors $K(\sqrt{aa_1})$ est de type $E_1'$ au-dessus de $k_1$, d'après le lemme 1, et réciproquement, si $K(\sqrt{b})$ est de type $E_1'$ au-dessus de $k_1$, $K(\sqrt{a_1 b})$ est de type $E_2'$.

Le théorème 10 résulte immédiatement de ce lemme et du théorème 9.

C. Q. F. D.

Remarque. - Les théorèmes précédents permettent de calculer explicitement le nombre des extensions galoisiennes de degré $p^3$ d'un corps local dont le groupe de Galois est d'un type donné (voir [7] ou [8]).

3.4. Description des classes admissibles. - Pour tout groupe abélien $G$, de type $(p , p)$, opérant trivialement sur $\mu_p$, on se propose de classifier les éléments de $H^2(G , \mu_p)$ en utilisant les théorèmes 6 à 10. On considèrera $H^2(G , \mu_p)$ comme un $\underset{\sim}{F}_p$-espace vectoriel, dont on sait (ou l'on démontre sans difficulté, en utilisant par exemple la suite exacte de Künneth, [2], p. 373) que la dimension est 3.

L'élément générique de $H^2(G , \mu_p)$ qui correspond à une extension de groupes de type $E_i$, $i = 0 , 1 , 2$ (resp. $E_j'$, $j = 1 , 2$), sera noté $\varepsilon_i$ (resp. $\varepsilon_j'$). Remarquons que les $\varepsilon_0$ sont les classes non nulles de $H^2(G , \mu_p)$ qui sont représentées par des cocycles symétriques.

3.4.1. Réalisation géométrique de $H^2(G , \mu_p)$ : Soit $P(K/k)$ un plan dégénéré, orthogonal à $\mu_p$. On voit facilement (théorème 5 et cas particulier 2.4) que $\dim \Gamma_K^G/\eta(\Gamma_k) = 3$. On en profite pour identifier $H^2(G , \mu_p)$ à $\Gamma_K^G/\eta(\Gamma_k)$ d'où, d'après les théorèmes 6 et 7 (resp. 8 à 10)

(i) La classe nulle et les classes $\varepsilon_0$ forment un plan de $H^2(G , \mu_p)$

(ii) Pour tout sous-groupe $J$ d'ordre $p$ de $G$, la suite :

$$0 \longrightarrow \operatorname{Ker} \operatorname{Res}_J \longrightarrow H^2(G , \mu_p) \xrightarrow{\operatorname{Res}_J} H^2(J , \mu_p) \longrightarrow 0 ,$$

où $\operatorname{Res}_J$ désigne la restriction à $J$, est exacte.

Donc $\dim \operatorname{Ker} \operatorname{Res}_J = 2$, i. e. $\operatorname{Ker} \operatorname{Res}_J$ est un plan de $H^2(G , \mu_p)$.

(iii) Tout plan $\operatorname{Ker} \operatorname{Res}_J$ contient une droite et une seule engendrée par une classe $\varepsilon_0$.

L'élément générique non nul de $\operatorname{Ker} \operatorname{Res}_J$ sera noté $\varepsilon_i(J)$ (resp. $\varepsilon_j'(J)$). Celui de $\operatorname{Ker} \operatorname{Res}_{J_1} \cap \operatorname{Ker} \operatorname{Res}_{J_2}$ sera noté $\varepsilon_i(J_1 , J_2)$ (resp. $\varepsilon_j'(J_1 , J_2)$).

(iv) Les classes $\varepsilon_1$ (resp. $\varepsilon_2'$) engendrent une droite de $H^2(G , \mu_p)$.

3.4.2. Caractérisation des classes admissibles : Rappelons qu'une classe $\varepsilon \in H^2(G , \mu_p)$ est dite admissible pour $K/k$ si le problème de plongement $(K/k , \varepsilon)$ admet une solution.

THÉORÈME 11. - Supposons $p \neq 2$

(i) Si $P(K/k)$ est dégénéré, orthogonal à $\mu_p$, toute classe est admissible.

(ii) Si $P(K/k)$ est dégénéré, non orthogonal à $\mu_p$, soit $J_1 = Gal(k_1/k)$, où $D(k_1/k)$ est la droite de $P(K/k)$ orthogonale à $\mu_p$. Les classes admissibles forment un plan de $H^2(G , \mu_p)$, confondu avec $\operatorname{Ker} \operatorname{Res}_{J_1}$. Les classes $\varepsilon_2(J_1)$ (resp. $\varepsilon_1$) engendrent une droite de ce plan.

(iii) Si $P(K/k)$ est non dégénéré, non orthogonal à $\mu_p$, aucune classe $\varepsilon_1$ n'est admissible. Soit $J_1$ défini comme dans (ii). Les classes admissibles forment un plan de $H^2(G , \mu_p)$, engendré par les classes $\varepsilon_2(J)$, $J$ parcourant l'ensemble des sous-groupes d'ordre $p$ de $G$ distincts de $J_1$. Une telle classe $\varepsilon_2(J)$ peut être caractérisée comme suit :

Soit $k_1 = k(\sqrt{\beta})$ le corps fixe de $J_1$. Soit $J_0$ un sous-groupe d'ordre $p$ de $G$, distinct de $J_1$ de corps fixe $k_0$. Soit $\xi$ l'unique élément de $\mu_p - \{1\}$ tel que $\xi^{-1} \beta \in N_{k_0/k} k_0^*$. Soit $\tau$ un générateur de $J_1$, et soit $\sigma$ le générateur de $J_0$ tel que $(\sqrt[p]{\beta})^{-1} \sigma(\sqrt[p]{\beta}) = \xi$. Pour qu'une classe $\varepsilon_2(J_0)$, décrivant une extension de groupes de type $E_2$, scindée par $J_0$, soit admissible, il faut et il suffit qu'elle soit représentée par un cocycle $a$ tel que

$$a(\sigma , \tau).a(\tau , \sigma)^{-1} = a(\tau^{p-1} , \tau).a(\tau^{p-2} , \tau) \dots a(\tau , \tau) .$$

(iv) Si $P(K/k)$ est non dégénéré, orthogonal à $\mu_p$, aucune classe $\varepsilon_i$ $(i=1,2)$ n'est admissible.

Démonstration. - Les assertions (i), (ii), (iv) sont immédiates à partir des théorèmes 6 et 7. Montrons (iii) :

Soit $L = K(\sqrt[p]{a})$ une extension de type $E_2$ au-dessus de $k_0$. On a vu (démonstration des théorèmes 7 et 8) qu'on peut prendre $a \in k_0^*$, avec $a^{-1}.\tau a = \lambda_0^p \beta$, $\lambda_0 \in k_0^*$. D'après 2.3, la classe décrivant l'extension est représentée par un cocycle $a(\sigma , \tau) = x_\sigma . \sigma(x_\tau) . x_{\sigma\tau}^{-1}$, et l'on peut prendre $x_\sigma = 1$, $x_\tau = \lambda_0 \sqrt[p]{\beta}$ (où $\sqrt[p]{\beta}$ représente une racine $p$-ième fixée de $\beta$). Alors

$$a(\sigma , \tau).a(\tau , \sigma)^{-1} = (\sqrt[p]{\beta})^{-1}.\sigma(\sqrt[p]{\beta}) = \xi .$$

Mais $\tau$ se prolonge à $L$ en posant $(\sqrt[p]{a})^{-1}.t(\sqrt[p]{a}) = x_\tau$ $t_K = \tau$, d'où

$$(\sqrt[p]{a})^{-1}.t^p(\sqrt[p]{a}) = x_\tau . \tau(x_\tau) \dots \tau^{p-1}(x_\tau) = N_\tau(x_\tau) .$$

Comme $N_\tau(x_\tau) = N_\tau(\lambda_0).\beta = \xi$, on en déduit, en identifiant $Gal(L/K)$ à $\mu_p$ par $t^p \longmapsto (\sqrt[p]{a})^{-1}.t^p(\sqrt[p]{a})$, la condition nécessaire :

$$a(\sigma , \tau).a(\tau , \sigma)^{-1} = t^p = a(\tau^{p-1} , \tau).a(\tau^{p-2} , \tau) \dots a(\tau , \tau) .$$

Cette condition est clairement suffisante (on construit l'extension $K(\sqrt[p]{a})$ comme dans la démonstration du théorème 7).

C. Q. F. D.

Remarque. - La condition (iii) redonne immédiatement celle donnée par GILLARD ([5], théorème 9) dans le cas modérément ramifié.

THÉORÈME 12. - Supposons que $p = 2$ .

(i) Si $P(K/k)$ est dégénéré, orthogonal à $-1$ , toute classe est admissible.

(ii) Si $P(K/k)$ est dégénéré, non orthogonal à $-1$ , soit $J_1 = \mathrm{Gal}(K/k_1)$ , où $D(k_1/k)$ est la droite de $P(K/k)$ orthogonale à $-1$ . Aucune classe $\varepsilon'_2$ n'est admissible. Les classes admissibles forment un plan, engendré par une classe $\varepsilon'_1(J_1)$ et une classe $\varepsilon_0(J_1)$ .

(iii) Si $P(K/k)$ est non dégénéré, non orthogonal à $-1$ , soit $J_1$ comme précédemment, et soient $J_2$ , $J_3$ les deux autres sous-groupes d'ordre 2 de $G$ . Les classes admissibles forment un plan, dont les trois vecteurs non nuls sont $\varepsilon_0(J_1)$ , $\varepsilon'_1(J_2 , J_3)$ et $\varepsilon'_2$ .

(iv) Dans tout autre cas, aucune classe $\varepsilon'_j$ $(j = 1 , 2)$ n'est admissible.

Démonstration. - Immédiate, à partir des théorèmes 8 à 10.

4. Enoncés globaux.

Soit $p$ un nombre premier. Soit $K/k$ une extension de corps de nombres contenant le groupe $\mu_p$ des racines $p$-ièmes de l'unité, abélienne de type $(p , p)$ . On a les critères suivants de plongement (comparer aux résultats de [4]).

THÉORÈME 13. - Supposons $p \neq 2$ . Soit $\xi_p$ une racine primitive $p$-ième de $1$ .

(i) Pour que $K/k$ se plonge dans une surextension galoisienne de type $E_1$ , il faut et il suffit que $K = k(\sqrt[p]{\alpha} , \sqrt[p]{\beta})$ , $\alpha \in k^*$ , $\beta \in k^*$ et $\beta$ est une norme de $k(\sqrt[p]{\alpha})$ à $k$

(ii) Pour que $K/k = k(\sqrt[p]{\alpha} , \sqrt[p]{\beta})/k$ se plonge dans une surextension galoisienne de type $E_2$ , non cyclique sur $k(\sqrt[p]{\alpha})$ , il faut et il suffit que :

- soit, $\beta$ et $\xi_p$ sont des normes de $k(\sqrt[p]{\alpha})$ à $k$

- soit, $\beta$ n'est pas une norme de $k(\sqrt[p]{\alpha})$ à $k$ , mais il existe $\xi \in \mu_p$ tel que $\xi^{-1}\beta$ est une norme de $k(\sqrt[p]{\alpha})$ à $k$ .

THÉORÈME 14. - Supposons $p = 2$ .

(i) Toute extension $K/k$ qui se plonge dans une surextension quaternionienne, se plonge aussi dans une extension diédrale.

(ii) Pour que $K/k = k(\sqrt{\alpha} , \sqrt{\beta})/k$ se plonge dans une surextension diédrale, cy-

clique sur $k(\sqrt{\alpha\beta})$ , il faut et il suffit que $\beta$ soit une norme de $k(\sqrt{\alpha})$ à k .

(iii) Dans les conditions de (ii), pour que K/k se plonge dans une surextension quaternionienne, il faut et il suffit que $-1$ soit une norme de $k(\sqrt{\alpha\beta})$ à k .

Démonstration. - Ces deux théorèmes résultent sans difficulté des parties des démonstrations des théorèmes 7 et 9 et des lemmes 1 et 2 qui sont d'ordre purement algébrique. On peut aussi regarder les conditions locales

BIBLIOGRAPHIE

[1] ARTIN (E.). - Algèbre géométrique. Traduit par M. Lazard. - Paris, Gauthier-Villars, 1962 (Cahiers scientifiques, 27).

[2] CARTAN (H.) and EILENBERG (S.). - Homological algebra. - Princeton, Princeton University Press, 1956 (Princeton mathematical Series, 19).

[3] CASSELS (J. W. S.) and FRÖHLICH (A.) [Editors]. - Algebraic number theory. Proceedings of an instructional conference of the London mathematical Society [1965. Brighton]. - London, Academic Press, 1967.

[4] DAMEY (P.) et PAYAN (J. J.). - Existence et construction des extensions galoisiennes de degré 8 d'un corps de caractéristique $\neq 2$ , J. reine und angew. Math., t. 244, 1970, p. 37-54.

[5] GILLARD (R.). - Plongement d'une extension d'ordre p ou $p^2$ dans une surextension non abélienne d'ordre $p^3$ , J. reine und angew. Math., t. 268/269, 1974, p. 418-426.

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

[7] MASSY (R.). - Les extensions galoisiennes de degré $p^3$ d'un corps $\mathcal{P}$-adique, Thèse 3e cycle, Math., Paris 1975.

[8] MASSY (R.) et NGUYEN-QUANG-DO (T.). - Extensions galoisiennes non abéliennes de degré $p^3$ d'un corps $\mathcal{P}$-adique, C. R. Acad. Sc. Paris, t. 280, 1975, Série A, p. 1345-1347.

(Texte reçu le 23 février 1976)

Richard MASSY
46 rue de Kermenguy
29200 BREST

et

Thong NGUYEN-QUANG-DO
49 rue Pierre Valette
92240 MALAKOFF