ANNALES SCIENTIFIQUES DE L'É.N.S.

JEAN-JACQUES PAYAN

Critère de décomposition d'une extension de Kummer sur un sous-corps du corps de base

Annales scientifiques de l'É.N.S. 4^e série, tome 1, n° 3 (1968), p. 445-458

<http://www.numdam.org/item?id=ASENS_1968_4_1_3_445_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 1, 1968, p. 445 à 458.

CRITÈRE DE DÉCOMPOSITION D'UNE EXTENSION DE KUMMER SUR UN SOUS-CORPS DU CORPS DE BASE

PAR JEAN-JACQUES PAYAN.

Dans ce qui suit G désigne un groupe abélien fini d'ordre e, d'exposant n et k un corps commutatif dont la caractéristique ne divise pas n. On suppose en outre que k contient les racines $n^{\text{ièmes}}$ de l'unité.

La première partie de ce travail est consacrée à l'étude de l'invariant de Hasse d'une extension de Kummer de k de groupe de Galois isomorphe à G. $\varkappa$ désignant un sous-corps de k tel que $k/\varkappa$ soit galoisienne, on étudie dans la seconde partie les extensions abéliennes N de k telles que $N/\varkappa$ soit galoisienne et $\mathrm{Gal}\,N/k$ isomorphe à G. La dernière partie est consacrée à la démonstration d'un critère explicite de décomposition sur $\varkappa$ d'une telle extension. Ce critère exprime en termes de cohomologie et précise les résultats de [4] et [6] dans le cas qui nous intéresse. Il met notamment en évidence le rôle joué par l'extension intermédiaire $\tilde{k}$ de $k/\varkappa$.

Ce dernier résultat est destiné à l'étude, généralisant celles de [2], [7], [8] et [9], de l'existence et des propriétés arithmétiques des extensions finies $K/\varkappa$ vérifiant la condition suivante : il existe une extension galoisienne k de $\varkappa$, contenant les racines $n^{\text{ièmes}}$ de l'unité, linéairement disjointe de K sur $\varkappa$, telle que la composée N de k et K soit galoisienne relativement à $\varkappa$ et $\mathrm{Gal}\,N/k$ isomorphe à G. Cette condition est vérifiée en particulier par les extensions abéliennes de $\varkappa$ de groupe de Galois isomorphe à G et linéairement disjointes sur $\varkappa$ du corps des racines $n^{\text{ièmes}}$ de l'unité. Cela explique pourquoi l'auteur s'est limité au cas des corps et n'a pas envisagé celui des algèbres abéliennes traité dans [6].

Je voudrais remercier Jean-Louis Koszul d'avoir eu la patience de m'écouter et Jean-Pierre Serre celle de lire mon premier manuscrit. Leurs

remarques et leurs suggestions ont considérablement facilité et clarifié la rédaction de ce travail.

1. Invariant de Hasse. — N désigne une extension abélienne de k dont le groupe de Galois est isomorphe à G. Si θ est un élément de N et σ un élément de G on notera θ^σ le transformé de θ par l'élément de Gal N/k dont l'image par l'isomorphisme est σ. X désignera le groupe des caractères de G à valeurs dans k^*. On notera $\langle \theta, \chi \rangle = \sum_{\sigma \in G} \chi(\sigma^{-1}) \theta^\sigma$ la résolvante de Lagrange associée à θ et χ.

Remarques :

1. Pour tout σ_0 de G on peut écrire

$$\langle \theta, \chi \rangle^{\sigma_0} = \chi(\sigma_0) \langle \theta, \chi \rangle.$$

2. Pour que les k-conjugués de θ forment une base de N/k — dite base normale — il faut et il suffit que

$$\prod_{\chi \in X} \langle \theta, \chi \rangle \in N^*.$$

Les éléments $\mathfrak{H}$ de N^* vérifiant $\mathfrak{H}^{1-\sigma} \in k^*$ pour tout σ de G forment un sous-groupe E de N^*. E peut également être défini comme l'ensemble des éléments de N^* dont la puissance $n^{\text{ième}}$ est dans k^*. L'application u qui à tout $\mathfrak{H}$ de E associe le caractère $\sigma \to \mathfrak{H}^{\sigma-1}$ est un homomorphisme de E sur X et la suite $0 \to k^* \to E \xrightarrow{u} X \to 0$ est exacte. On le démontre facilement à l'aide du théorème de la base normale (*cf.* [1]) et en remarquant que tout élément de E est de la forme $\lambda \langle \theta, \chi \rangle$ où $\lambda \in k^*$ et où les conjugués de θ forment une base de N/k (*cf.* [2] et [4]). E est donc une extension de k^* par X, on peut lui associer un élément de $H^2(X, k^*)$ [ou de $\mathrm{Ext}^1(X, k^*)$ puisque tous les groupes considérés sont abéliens], cet élément est d'ailleurs la classe du 2-cocycle défini par

$$\chi, \chi' \to \frac{\langle \theta, \chi \rangle \langle \theta, \chi' \rangle}{\langle \theta, \chi\chi' \rangle}.$$

On peut remplacer u par son composé avec un élément arbitraire de Aut X, ce qui nous conduit pour éviter l'identification de G à Gal N/k gênante dans les questions d'existence à définir l'invariant de Hasse de la façon suivante [Aut X opère sur $H^2(X, k^*)$ et $\mathrm{Ext}^1(X, k^*)$ de façon évidente]:

Définition 1. — On appellera *invariant de Hasse* de N/k la trajectoire de Aut X dans $H^2(X, k^*)$ engendrée par la classe du 2-cocycle $\chi, \chi' \to \frac{\langle \theta, \chi \rangle \langle \theta, \chi' \rangle}{\langle \theta, \chi\chi' \rangle}$ où les conjugués de θ forment une base normale de N/k.

En élevant à l'exposant n la suite exacte précédente en donne une nouvelle que nous écrirons

$$0 \to k^{\star n} \to E^n \xrightarrow{u'} X \to 0.$$

Le groupe E^n est une extension de $k^{\star n}$ par X contenue dans $k^\star$ (puisque les $\langle \theta, \chi \rangle^n$ sont invariants par les éléments de $\mathrm{Gal}\, N/k$).

Réciproquement si E′ désigne une extension de $k^{\star n}$ par X contenue dans $k^\star$, on sait (*cf.* [4] ou exercices de [1]) que l'extension N/k obtenue par adjonction à k des racines $n^{\text{ièmes}}$ des éléments de E′ est abélienne et que son groupe de Galois est isomorphe à G. La correspondance ainsi définie entre les sous-groupes de $k^\star$ extensions de $k^{\star n}$ par X et les extensions abéliennes de k de groupe de Galois isomorphe à G est bijective.

Il reste à caractériser les trajectoires de Aut X dans $H^2(X, k^\star)$ qui sont des invariants de Hasse. Après avoir remarqué que les 2-cocycles $\chi, \chi' \to \dfrac{\langle \theta, \chi \rangle \langle \theta, \chi' \rangle}{\langle \theta, \chi\chi' \rangle}$ sont symétriques, on notera $\overline{Z}^2(X, k^\star)$ [resp. $\overline{H}^2(X, k^\star)$] l'ensemble des 2-cocycles symétriques [resp. des éléments de $H^2(X, k^\star)$ engendrés par les 2-cocycles symétriques]. $\overline{H}^2(X, k^\star)$ et $\mathrm{Ext}^1(X, k^\star)$ sont évidemment isomorphes.

Définition 2. — Si μ appartient à $Z^2(X, k^\star)$ et si Y est un sous-groupe de X on dira que μ se *décompose* sur Y si $\mu \mid Y^2$ appartient à $B^2(Y, k^\star)$. On dira que μ est irréductible s'il ne se décompose sur aucun sous-groupe de X distinct de l'élément neutre. Une trajectoire de Aut X dans $\overline{H}^2(X, k^\star)$ est dite irréductible si elle est définie à partir d'un 2-cocycle irréductible.

Pour caractériser les invariants de Hasse nous aurons besoin des lemmes suivants :

Lemme 1. — *Pour tout couple χ, χ' d'éléments de* X *et tout élément μ de $\overline{Z}^2(X, k^\star)$ on peut écrire*

$$\prod_{p=1}^{n} \frac{\mu(\chi, \chi^p)\, \mu(\chi', \chi'^p)}{\mu(\chi\chi', \chi^p \chi'^p)} = \mu(\chi, \chi')^n,$$

μ étant un 2-cocycle on peut écrire quels que soient les caractères χ_1, χ_2 et χ_3 :

$$\mu(\chi_1, \chi_2)\, \mu(\chi_1 \chi_2, \chi_3) = \mu(\chi_1, \chi_2 \chi_3)\, \mu(\chi_2, \chi_3). \tag{E}$$

Le lemme sera démontré si nous pouvons établir que

$$\frac{\mu(\chi, \chi^p)\, \mu(\chi', \chi'^p)}{\mu(\chi\chi', \chi^p \chi'^p)} = \frac{\mu(\chi, \chi')\, \mu(\chi^p, \chi'^p)}{\mu(\chi^{p+1}, \chi'^{p+1})}. \tag{1}$$

En remplaçant χ_1 par χ, χ_2 par χ' et χ_3 par $\chi^p\chi'^p$ dans (E), on voit que (1) équivaut à

$$(1') \qquad \frac{\mu(\chi, \chi^p)\,\mu(\chi', \chi'^p)}{\mu(\chi', \chi^p\chi'^p)} = \frac{\mu(\chi, \chi^p\chi'^{p+1})\,\mu(\chi^p, \chi'^p)}{\mu(\chi^{p+1}, \chi'^{p+1})}.$$

En substituant χ à χ_1, χ^p à χ_2 et χ'^{p+1} à χ_3 on voit que (1') équivaut à

$$(1'') \qquad \mu(\chi', \chi'^p)\,\mu(\chi^p, \chi'^{p+1}) = \mu(\chi^p, \chi'^p)\,\mu(\chi', \chi^p\chi'^p)$$

qui résulte de (E) en y remplaçant χ_1 par χ', χ_2 par χ'^p et χ_3 par χ^p et en utilisant la symétrie sur $\mu(\chi^p, \chi'^{p+1})$.

Lemme 2. — *Si Y_1 et Y_2 sont des sous-groupes de* X *dont l'intersection se réduit à l'élément neutre et si μ se décompose sur* Y_1 *et sur* Y_2, *il se décompose sur* $Y_1 Y_2$.

Les hypothèses entraînent l'existence d'une application ρ_1 (resp. ρ_2) de Y_1 (resp. Y_2) dans k^* telle que pour tout couple de caractères χ, χ' de Y_1 (resp. Y_2) :

$$\mu(\chi, \chi') = \frac{\rho_1(\chi)\,\rho_1(\chi')}{\rho_1(\chi\chi')} \qquad \left[\text{resp. } \mu(\chi, \chi') = \frac{\rho_2(\chi)\,\rho_2(\chi')}{\rho_2(\chi\chi')}\right]$$

de plus, $\rho_1(1) = \rho_2(1) = \mu(1, \chi)$.

Si χ appartient à $Y_1 Y_2$ il s'écrit d'une façon et d'une seule sous la forme $\chi = \chi_1\chi_2$ avec $\chi_1 \in Y_1$ et $\chi_2 \in Y_2$. Posons

$$\rho(\chi) = \frac{\rho_1(\chi_1)\,\rho_2(\chi_2)}{\mu(\chi_1, \chi_2)}.$$

On définit ainsi une application $\rho : Y_1 Y_2 \to k^*$ dont les restrictions respectives à Y_1 et Y_2 sont ρ_1 et ρ_2. Considérons alors un couple d'élément χ, χ' de $Y_1 Y_2$, ils s'écrivent $\chi = \chi_1\chi_2$ et $\chi' = \chi'_1\chi'_2$ avec χ_1 et $\chi'_1 \in Y_1$ et χ_2 et $\chi'_2 \in Y_2$. En utilisant le fait que μ est symétrique, on peut écrire

$$\mu(\chi_1, \chi_2)\,\mu(\chi_1\chi_2, \chi'_1\chi'_2) = \mu(\chi_1, \chi'_1\chi_2\chi'_2)\,\mu(\chi_2, \chi'_1\chi'_2)$$

et

$$\mu(\chi'_1, \chi_2)\,\mu(\chi'_1\chi'_2, \chi_2) = \mu(\chi'_1, \chi_2\chi'_2)\,\mu(\chi_2, \chi'_2)$$

et

$$\mu(\chi'_1, \chi_2\chi'_2)\,\mu(\chi'_1\chi_2\chi'_2, \chi_1) = \mu(\chi_1, \chi'_1)\,\mu(\chi_1\chi'_1, \chi_2\chi'_2),$$

ce qui entraîne immédiatement

$$\mu(\chi, \chi') = \frac{\mu(\chi_1, \chi'_1)\,\mu(\chi_2, \chi'_2)\,\mu(\chi_1\chi'_1, \chi_2\chi'_2)}{\mu(\chi_1, \chi_2)\,\mu(\chi'_1, \chi'_2)}$$

et compte tenu de la définition de ρ, on en déduit

$$\mu(\chi, \chi') = \frac{\rho(\chi_1\chi_2)\,\rho(\chi_1'\chi_2')}{\rho(\chi_1\chi_1'\chi_2\chi_2')} = \frac{\rho(\chi)\,\rho(\chi')}{\rho(\chi\chi')}$$

qui achève la démonstration.

LEMME 3. — *Soit* $\mu \in \overline{Z}(X, k^*)$, *si* Y *est un sous-groupe d'exposant* m *de* X *tel que pour tout caractère* χ *de* Y *on ait :*

$$\prod_{p=1}^{m} \mu(\chi, \chi^p) \in k^{*m},$$

alors μ *se décompose sur* Y.

Montrons que c'est vrai si Y est cyclique et engendré par χ_0. Dans ce cas, on pose $\rho(1) = \mu(1, \chi)$ et on choisit pour $\rho(\chi_0)$ une des racines $m^{\text{ièmes}}$ de $\prod_{p=1}^{m} \mu(\chi_0, \chi_0^p)$. On définit alors de proche en proche $\rho(\chi_0^p)$ à l'aide de l'égalité

$$\rho(\chi_0^p) = \frac{\rho(\chi_0)\,\rho(\chi_0^{p-1})}{\mu(\chi_0, \chi_0^{p-1})}.$$

De l'égalité

$$\mu(\chi_0^p, \chi_0^q)\,\mu(\chi_0^{p+q}, \chi_0) = \mu(\chi_0^p, \chi_0^{q+1})\,\mu(\chi_0^q, \chi_0)$$

on déduit facilement que

$$\mu(\chi_0^p, \chi_0^q) = \frac{\rho(\chi_0^p)\,\rho(\chi_0^q)}{\rho(\chi_0^{p+q})}$$

qui signifie que μ se décompose sur Y.

Supposons que la proposition est vraie si Y est produit direct de $(r-1)$ groupes cycliques. Le lemme 2 entraînera sa validité pour un produit de r groupes cycliques.

Nous pouvons alors énoncer :

THÉORÈME I (à rapprocher du théorème 4 de [4]). — *Il y a correspondance biunivoque entre les trajectoires irréductibles de* Aut X *dans* $\overline{H}^2(X, k^*)$ $[\simeq \mathrm{Ext}^1(X, k^*)]$ *et les extensions abéliennes de* k *de groupe de Galois isomorphe à* G. *Les premières sont les invariants de Hasse des secondes.*

Montrons que si N/k est abélienne et Gal N/k isomorphe à G l'invariant de Hasse de N/k est une trajectoire irréductible. Notons μ_0 le 2-cocycle $\chi, \chi' \to \frac{\langle \theta, \chi\rangle\langle \theta, \chi'\rangle}{\langle \theta, \chi\chi'\rangle}$ et supposons que μ_0 se décompose sur un sous-groupe

Y de X, c'est-à-dire qu'il existe une application ρ de Y dans k^* telle que pour tout couple de caractères χ, χ' de Y, on ait

$$\mu_\theta(\chi, \chi') = \frac{\rho(\chi)\,\rho(\chi')}{\rho(\chi\chi')},$$

on en déduirait que pour tout χ de Y :

$$\prod_{q=1}^{n} \mu_\theta(\chi, \chi^p) = \langle \theta, \chi \rangle^n = \rho(\chi)^n$$

qui entraîne $\langle \theta, \chi \rangle = \lambda \langle \theta, 1 \rangle$ où $\lambda \in k^*$ [$\langle \theta, 1 \rangle = \mathrm{Tr}_{N/k}\theta$ est évidemment dans k^*]. Cette dernière égalité s'écrit

$$\sum_{\sigma \in G} (\chi(\sigma^{-1}) - \lambda)\,\theta^\sigma = 0;$$

l'indépendance des θ^σ sur k entraîne $\lambda = 1$ et $\chi = 1$; c'est-à-dire que Y se réduit à l'élément neutre, μ_θ est donc irréductible.

Considérons maintenant un 2-cocycle irréductible μ et la trajectoire irréductible de Aut X qu'il engendre. Nous allons construire le groupe E^n. Le sous-groupe E' de k^* engendré par k^{*n} et les éléments $\prod_{p=1}^{n} \mu(\chi, \chi^p)$ où χ parcourt X est une extension de k^{*n} par X. Il suffit pour le montrer de prouver que l'application $\Phi : X \to k^*/k^{*n}$ définie par

$$\Phi(\chi) = k^{*n} \prod_{p=1}^{n} \mu(\chi, \chi^p)$$

est un homomorphisme injectif. Le lemme 1 montre que Φ est un homomorphisme, le lemme 3 montre que μ se décompose sur $\mathrm{Ker}\Phi$ comme μ est irréductible, il en résulte que $\mathrm{Ker}\Phi$ se réduit à l'élément neutre de X donc que Φ est injectif. En prenant l'extension N de k engendrée par les racines $n^{\text{ièmes}}$ des éléments de E' on voit que la trajectoire irréductible considérée est l'invariant de Hasse de N/k et que $E^n = E'$.

θ désignant encore un élément de N dont les conjugués forment une base de N/k nous aurons besoin du résultat suivant :

THÉORÈME II. — *L'application qui à chaque élément $\mathfrak{S}$ d'une base normale de N/k associe le 2-cocycle $\mu_\mathfrak{S}$:*

$$\chi, \chi' \to \frac{\langle \mathfrak{S}, \chi \rangle \langle \mathfrak{S}, \chi' \rangle}{\langle \mathfrak{S}, \chi\chi' \rangle}$$

définit une application biunivoque entre les bases normales de N/k et les 2-cocycles équivalents à μ_θ.

Tout élément ϑ de N s'écrit $\vartheta = \sum_{\sigma \in G} \lambda_\sigma \theta^\sigma$ dont on déduit

$$\langle \vartheta, \chi \rangle = \langle \theta, \chi \rangle \sum_{\sigma \in G} \lambda_\sigma \chi(\sigma).$$

Il en résulte que

$$\mu_\vartheta(\chi, \chi') = \frac{\rho(\chi)\,\rho(\chi')}{\rho(\chi\chi')}\,\mu_\theta(\chi, \chi')$$

où on a posé

$$\rho(\chi) = \sum_{\sigma \in G} \lambda_\sigma \chi(\sigma) \quad \text{pour tout } \chi \text{ de X.}$$

Réciproquement, si l'on considère un 2-cocycle μ équivalent à μ_θ

$$\Leftrightarrow \mu(\chi, \chi') = \frac{\rho(\chi)\,\rho(\chi')}{\rho(\chi\chi')}\,\mu_\theta(\chi, \chi')$$

pour tous les χ, χ' de X il existe ϑ dont les conjugués forment une base de N/k et vérifiant $\mu = \mu_\vartheta$. Un tel ϑ est donné par le système de Cramer :

$$\sum_{\sigma \in G} \lambda_\sigma \chi(\sigma) = \rho(\chi) \quad \text{pour tout } \chi \text{ de X.}$$

Pour obtenir tous les ϑ tels que $\mu_\vartheta = \mu$ il suffit de remarquer que l'application ρ est déterminée au produit près par un caractère de X donc que les autres solutions seront données par les systèmes $\sum \lambda'_\sigma \chi(\sigma) = \rho(\chi)\,\chi(\sigma_0)$ où σ_0 parcourt G. On en déduit

$$\sum_{\sigma \in G} \lambda'_\sigma \chi(\sigma) = \chi(\sigma_0) \sum_{\sigma \in G} \lambda_\sigma \chi(\sigma) \quad \text{pour tout } \chi$$

soit encore

$$\sum_{\sigma \in G} \lambda'_\sigma \chi(\sigma) = \sum_{\sigma \in G} \lambda_{\sigma\sigma_0^{-1}} \chi(\sigma)$$

qui donne $\lambda'_\sigma = \lambda_{\sigma\sigma_0^{-1}}$ pour tout σ_0, soit encore $\vartheta = \vartheta^{\sigma_0}$ qui achève la démonstration.

Dorénavant, nous noterons $\mathfrak{H}$ l'invariant de Hasse d'une extension abélienne N/k, E^n l'extension de k^{*n} par X contenue dans k^* qui lui est associée et nous poserons $W = E^n/k^{*n}$.

2. Extensions de Kummer de k galoisiennes sur un sous-corps $\varkappa$ de k. — On suppose dorénavant que k est une extension galoisienne, pas nécessairement finie, d'un corps $\varkappa$ et l'on pose $g = \mathrm{Gal}\, k/\varkappa$. On se propose d'étudier les extensions abéliennes N de k galoisiennes sur $\varkappa$ telles que $\mathrm{Gal}\, N/k$ soit isomorphe à G. On posera alors $\mathrm{Gal}\, N/\varkappa = \mathfrak{G}$. Quand

l'extension N/k sera donnée ainsi que l'isomorphisme de G sur $\mathrm{Gal}\,N/k$ on identifiera ces deux groupes.

On sait (*cf.* [4], p. 36) que $N/\varkappa$ est galoisienne si et seulement si W est globalement invariant par les éléments de g, ce qui s'exprime en disant que g opère sur W. Comme g opère à gauche de façon évidente sur $\overline{H}^2(X, k^*)$ on peut traduire la propriété précédente par le :

LEMME 4. — *Pour que* $N/\varkappa$ *soit galoisienne il faut et il suffit que* g *opère sur son invariant de Hasse* $\mathfrak{H}$ *donc sur* E^n.

Nous dirons quand un risque de confusion se présentera que g opère par Galois.

Nous noterons désormais $\varkappa_n$ l'extension de $\varkappa$ obtenue en lui adjoignant les racines $n^{\text{ièmes}}$ de l'unité. $\mathrm{Gal}\,\varkappa_n/\varkappa$ est canoniquement isomorphe à un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$ et la restriction des éléments de g à $\varkappa_n$ est un homomorphisme de g sur $\mathrm{Gal}\,\varkappa_n/\varkappa$. On notera t l'élément de $(\mathbf{Z}/n\mathbf{Z})^*$ image de τ de g par cet homomorphisme canonique. Si α est un élément d'un groupe abélien H d'exposant n on fait opérer g à gauche sur H en posant $\tau(\alpha) = \alpha^t$. Nous utiliserons les cas $H = k^*/k^{*n}$, $H = X$, $H = \mathfrak{H}$ et $H = W$ et nous dirons alors que g opère naturellement.

A chaque extension $\mathfrak{G}$ de G par g correspond un homomorphisme φ de g dans AutG défini par $\sigma \to \varphi(\tau)\,\sigma = \bar{\tau}\sigma\bar{\tau}^{-1}$ où $\bar{\tau}$ désigne un relèvement de τ dans $\mathfrak{G}$. Réciproquement si l'on se donne un homomorphisme φ de g dans AutG, les classes d'extensions de G par g auxquelles il est associé correspondent biunivoquement aux éléments de $H^2(g, G)$ (*cf.* [10]).

Étant donné un homomorphisme φ de g dans AutG on lui associe l'homomorphisme Φ de g dans AutX défini comme suit : à τ de g et χ de X on associe le caractère $\Phi(\tau)\chi$ défini par

$$\Phi(\tau)\,\chi(\sigma) = \chi^{t^{-1}}[\varphi(\tau)\,\sigma].$$

Si l'on pose ${}^{\tau_\Phi}\mu(\chi, \chi') = \mu(\Phi(\tau^{-1})\chi, \Phi(\tau^{-1})\chi')$ on fait opérer à gauche g sur $Z^2(X, k^*)$, et $B^2(X, k^*)$ est invariant, on peut donc passer au quotient et faire opérer g à gauche sur $\overline{H}^2(X, k^*)$ et également sur le sous-groupe W de k^*/k^{*n} associé à un invariant de Hasse, nous dirons alors que g opère par Φ.

Nous pouvons alors énoncer :

THÉORÈME III. — *g opère compatiblement par Galois et par Φ sur $\mathfrak{H}$ et W. Cela définit l'homomorphisme φ associé à $\mathfrak{G}$. Pour que $\mathfrak{G}$ soit une extension centrale de G il faut et il suffit que g opère compatiblement par Galois et par l'opération naturelle sur $\mathfrak{H}$ et W.*

Le théorème I montre qu'il suffit de faire la démonstration pour les opérations de g sur $\mathfrak{H}$. Soit θ un élément de N dont les k-conjugués forment une base normale, la première assertion revient à prouver que pour tout τ de g les 2-cocycles μ_θ^τ et $\tau_\Phi . \mu_\theta$ sont équivalents.

Par définition

$$\tau_\Phi \mu_\theta(\chi, \chi') = \frac{\langle \theta, \Phi(\tau^{-1})\chi\rangle \langle \theta, \Phi(\tau^{-1})\chi'\rangle}{\langle \theta, \Phi(\tau^{-1})\chi\chi'\rangle}.$$

Si $\bar{\tau}$ est un élément de $\mathfrak{G}$ dont la restriction à k est égale à τ, on peut écrire

$$\mu_\theta(\chi, \chi')^\tau = \frac{\langle \theta, \chi\rangle^{\bar{\tau}} \langle \theta, \chi'\rangle^{\bar{\tau}}}{\langle \theta, \chi\chi'\rangle^{\bar{\tau}}}.$$

Mais

$$\langle \theta, \chi\rangle^{\bar{\tau}} = \sum_{\sigma \in G} [\chi(\sigma^{-1})]^\tau \theta^{\bar{\tau}\sigma},$$

après avoir posé $\sigma' = \bar{\tau}\sigma\bar{\tau}^{-1} = \varphi(\tau)\sigma$, on obtient

$$\langle \theta, \chi\rangle^{\bar{\tau}} = \sum_{\sigma' \in G} \chi^t(\varphi(\tau^{-1})\sigma'^{-1})\, \theta^{\sigma'\bar{\tau}} = \langle \theta^{\bar{\tau}}, \Phi(\tau^{-1})\chi\rangle.$$

Comme (*cf.* remarque 1) $\dfrac{\langle \theta, \Phi(\tau^{-1})\chi\rangle}{\langle \theta^{\bar{\tau}}, \Phi(\tau^{-1})\chi\rangle}$ est dans k^*, il en résulte que μ_θ^τ et $\tau_\Phi . \mu_\theta$ sont équivalents.

Rappelons que $\mathfrak{G}$ est dite extension centrale de G si G est contenu dans le centre de $\mathfrak{G}$. Compte tenu de ce que nous venons de montrer la seconde assertion revient à montrer que l'opération naturelle de g et celle qui est définie par Φ sont compatibles sur $\mathfrak{H}$ et W.

Cela se traduit par : pour tout χ de X et tout τ de g, $\Phi(\tau^{-1})\chi = \chi^t$, en revenant à la définition de Φ on voit que cela signifie que φ est l'homomorphisme trivial ou encore que pour tout relèvement $\bar{\tau}$ de τ dans $\mathfrak{G}$: $\bar{\tau}\sigma\bar{\tau}^{-1} = \sigma$. Cette seconde assertion n'est qu'une généralisation de l'énoncé de [4], p. 11.

3. Extensions décomposées. — N désignera encore une extension abélienne de k de groupe de Galois isomorphe à G, $\mathfrak{H}$ son invariant de Hasse, W et E^n les sous-groupes de k^*/k^{*n} et k^* qui lui sont canoniquement associés.

Si $N/\varkappa$ est galoisienne, l'extension $\mathfrak{G}$ de G par g est dite décomposée ou encore produit semi-direct de G par g s'il existe un relèvement $\bar{g}$ de g dans $\mathfrak{G}$, c'est-à-dire s'il existe une section de g qui soit un homomorphisme

(*cf.* [9]). Si $\mathfrak{G}$ et g sont munis, dans le cas g infini, de la topologie de Krull définie à l'aide des sous-groupes distingués d'indice fini, on voit facilement que la projection de $\mathfrak{G}$ sur g est continue et ouverte donc que $\bar{g}$ est ouvert. Dire que $\mathfrak{G}$ est décomposée signifie que N est composée de k et d'une extension K de $\varkappa$, K et k étant linéairement disjointes sur $\varkappa$. Il suffit pour le voir de prendre pour K l'extension intermédiaire de $N/\varkappa$ qui appartient à $\bar{g}$.

Nous avons vu (*cf.* théorème III) que si $N/\varkappa$ était galoisienne on lui associait un homomorphisme Φ de g dans Aut X avec lequel on faisait opérer g à gauche sur $\mathfrak{H}$, W, k^{*X} et k^{*X^2}. Nous noterons désormais $\tau\alpha$ l'image d'un α de W (resp. $\mathfrak{H}$, resp. k^{*X}, resp. k^{*X^2}) obtenue en faisant opérer g par Φ. On désignera dorénavant par $\tilde{k}$ l'extension intermédiaire de $k/\varkappa$ qui appartient à $\ker\Phi$. Comme $\ker\Phi$ est un sous-groupe distingué et d'indice fini de g, $\tilde{k}/\varkappa$ est galoisienne et finie.

Dans ce qui suit nous utiliserons les bi-g-modules k^{*X}, k^{*X^2} et $\mathbf{Z}^1(X, k^*)$, g opérant à gauche par Galois et par Φ et les deux premiers groupes de cohomologie qui leurs sont associés (*cf.* [3]).

C'est ainsi qu'un élément de $\mathbf{Z}^0[g, k^{*X}]$ sera un élément ρ de k^{*X} vérifiant pour tout τ de g : $\rho^\tau = \tau\rho$; qu'un élément u de $B^1[g, k^{*X}]$ sera défini à partir d'un ρ de k^{*X} par l'équation $u(\tau) = \frac{\rho^\tau}{\tau\rho}$ et qu'enfin un élément φ de $\mathbf{Z}^1[g, k^{*X}]$ est une application de g dans k^{*X} vérifiant pour tout couple d'éléments τ et τ' de g :

$$\delta\varphi(\tau, \tau') = \frac{\varphi(\tau')^\tau . \tau'\varphi(\tau)}{\varphi(\tau\tau')} = 1,$$

où δ désigne l'opération cobord.

Si $N/\varkappa$ est décomposée nous utiliserons les bases normales de N/k formées des conjugués d'un élément de K, le lemme suivant précise comment les obtenir :

LEMME 5. — *Il existe* θ *de* K *dont les* k*-conjugués forment une base de* N/k. *Il y a une correspondance biunivoque entre les* $\mathfrak{H}$ *de* K *dont les* k*-conjugués forment une base de* N/k *et les éléments de* $\mathbf{Z}^0(g, k^{*X})$.

Pour démontrer la première assertion remarquons que si $K/\varkappa$ est galoisienne, elle possède une base normale, l'indépendance linéaire de K et k sur $\varkappa$ montre que cette base est une base normale de N/k. Si $K/\varkappa$ n'est pas galoisienne alors $\varkappa$ est infini car toute extension finie d'un corps fini est cyclique. Une adaptation immédiate de la démonstration qui figure dans [1] du théorème de la base normale entraîne le résultat cherché.

$\{\theta^\sigma\}_{\sigma\in G}$ désignera une telle base, soit alors $\vartheta = \sum_{\sigma\in G} \lambda_\sigma \theta^\sigma$ un élément de N, on pose

$$\rho(\chi) = \sum_{\sigma\in G} \lambda_\sigma \chi(\sigma) = \frac{\langle \vartheta, \chi\rangle}{\langle \theta, \chi\rangle}$$

et on note encore $\bar{g}$ le relèvement de g auquel appartient K et $\bar{\tau}$ le relèvement dans $\bar{g}$ d'un élément τ de g.

Supposons que $\vartheta \in K$ et que les k-conjugués de ϑ forment une base de N/k : $\chi \to \rho(\chi)$ est alors une application de X dans k^* et on peut écrire pour tout τ de g :

$$\begin{aligned}\langle \vartheta, \chi\rangle^{\bar{\tau}} &= \langle \vartheta, \Phi(\tau^{-1})\chi\rangle = \tau\rho(\chi)\langle \theta, \Phi(\tau^{-1})\chi\rangle \\ &= [\rho(\chi)\langle \theta, \chi\rangle]^{\bar{\tau}} = \rho(\chi)^\tau \langle \theta, \Phi(\tau^{-1})\chi\rangle,\end{aligned}$$

d'où

$$\tau\rho(\chi) = \rho(\chi)^\tau \iff \rho \in Z^0(g, k^{*X}).$$

Réciproquement, considérons $\rho \in Z^0(g, k^{*X})$, le nombre ϑ de N défini par $\vartheta = \frac{1}{e}\sum_{\chi\in X} \rho(\chi)\langle \theta, \chi\rangle$ vérifie $\langle \vartheta, \chi\rangle = \rho(\chi)\langle \theta, \chi\rangle$ pour tout χ de X. En outre

$$\vartheta^{\bar{\tau}} = \frac{1}{e}\sum_{\chi\in X} \rho(\chi)^\tau \langle \theta, \chi\rangle^{\bar{\tau}} = \frac{1}{e}\sum_{\chi\in X} \rho(\chi)^\tau \langle \theta, \Phi(\tau^{-1})\chi\rangle.$$

compte tenu de $\rho^\tau = \tau\rho$, on en déduit

$$\vartheta^{\bar{\tau}} = \frac{1}{e}\sum_{\Phi(\tau^{-1})\chi\in X} \rho(\Phi(\tau^{-1})\chi)\langle \theta, \Phi(\tau^{-1})\chi\rangle = \vartheta,$$

d'où résulte que $\vartheta \in K$ et que ses conjugués forment une base de N/k.

Remarque 3 :

$$Z^0(g, k^{*X}) \subset \mathcal{J}^{*X}.$$

Nous avons vu dans la démonstration du théorème III que si μ est un 2-cocycle qui engendre $\mathfrak{H}$, son cobord $\tau \to \frac{\mu^\tau}{\tau\mu}$ est une application de g dans $B^2(X, k^*)$, nous allons étudier cette propriété de plus près.

Soit encore N une extension de k de groupe de Galois G, galoisienne sur k et Φ l'homomorphisme de g dans Aut X qui lui est associé. On note encore δ l'opération cobord qui à $\mu \in \bar{Z}^2(X, k^*)$ associe

$$\left(\tau \to \frac{\mu^\tau}{\tau\mu}\right) \in B^1[g, Z^2(X, k^*)].$$

Nous allons démontrer le

THÉORÈME IV. — *Soit μ un 2-cocycle irréductible qui engendre l'invariant de Hasse $\mathfrak{H}$ associé à* N, *alors*

$$\delta\mu \in B^1[g, \mathbf{Z}^2(X, k^*)] \cap \mathbf{Z}^1[g, B^2(X, k^*)].$$

Pour que $N/\varkappa$ *soit décomposée il faut et il suffit que* $\delta\mu \in B^1[g, B^2(X, k^*)]$.

La première assertion résulte immédiatement de ce qui a été rappelé ci-dessus. Pour démontrer la seconde, remarquons que si $N/\varkappa$ est décomposée et si θ est un élément de K vérifiant les conditions du lemme 5 alors $\mu_\theta^\tau = \tau\mu_\theta$. $\left(\text{On pose toujours } \mu_\theta : \chi, \chi' \to \frac{\langle\theta, \chi\rangle\langle\theta, \chi'\rangle}{\langle\theta, \chi\chi'\rangle}.\right)$ Comme les 2-cocycles qui engendrent $\mathfrak{H}$ sont au produit près par un 2-cobord de la forme $\chi, \chi' \to \mu_\theta[u(\chi), u(\chi')]$ où $u \in \mathrm{Aut}\, X$, la condition nécessaire est démontrée. Supposons réciproquement que

$$\tau \to \frac{\mu^\tau}{\tau\mu} \in B^1[g, B^2(X, k^*)],$$

il en résulte que si θ est un élément d'une base normale de N/k,

$$\tau \to \frac{\mu_\theta^\tau}{\tau\mu_\theta} \in B^1[g, B^2(X, k^*)],$$

ce qui s'exprime par l'existence de $\rho \in k^{*X}$ tel que

$$\frac{\mu_\theta(\chi, \chi')^\tau}{\mu_\theta(\Phi(\tau^{-1})\chi, \Phi(\tau^{-1})\chi')} = \frac{\rho(\chi)^\tau \rho(\chi')^\tau \rho(\Phi(\tau^{-1})\chi\chi')}{\rho(\Phi(\tau^{-1})\chi)\rho(\Phi(\tau^{-1})\chi')\rho(\chi\chi')^\tau}$$

en considérant le $\mathfrak{I}$ de N défini par $\rho(\chi)\langle\mathfrak{I}, \chi\rangle = \langle\theta, \chi\rangle$ pour tout χ de X, on voit que $\mu_{\mathfrak{I}}^\tau = \tau\mu_{\mathfrak{I}}$ pour tout τ de g.

Soit alors τ' un relèvement de τ dans $\mathfrak{G}$. On peut écrire

$$\left(\frac{\langle\mathfrak{I}, \chi\rangle\langle\mathfrak{I}, \chi'\rangle}{\langle\mathfrak{I}, \chi\chi'\rangle}\right)^\tau = \frac{\langle\mathfrak{I}, \chi\rangle^{\tau'}\langle\mathfrak{I}, \chi'\rangle^{\tau'}}{\langle\mathfrak{I}, \chi\chi'\rangle}$$

$$= \frac{\langle\mathfrak{I}^{\tau'}, \Phi(\tau^{-1})\chi\rangle\langle\mathfrak{I}^{\tau'}, \Phi(\tau^{-1})\chi'\rangle}{\langle\mathfrak{I}^{\tau'}, \Phi(\tau^{-1})\chi\chi'\rangle} = \frac{\langle\mathfrak{I}, \Phi(\tau^{-1})\chi\rangle\langle\mathfrak{I}, \Phi(\tau^{-1})\chi'\rangle}{\langle\mathfrak{I}, \Phi(\tau^{-1})\chi\chi'\rangle}$$

pour tous les χ, χ' de X. Le théorème II montre que $\mathfrak{I}$ et $\mathfrak{I}^{\tau'}$ sont alors k-conjugués, on peut donc en multipliant au besoin τ' par un élément convenable de G trouver un relèvement $\bar{\tau}$ de τ dans $\mathfrak{G}$ tel que $\mathfrak{I} = \mathfrak{I}^{\bar{\tau}}$. L'application $\tau \to \bar{\tau}$ est un relèvement de g dans $\mathfrak{G}$ et $\mathfrak{G}$ est donc décomposée.

Si n_χ désigne l'ordre de χ dans X nous poserons $n = n_\chi . f_\chi$ et nous dirons qu'une application α de X dans k^* représente proprement W si $\chi \to \alpha(\chi)^{f_\chi} . k^{*n}$ est un isomorphisme de X sur W et si pour tout τ de g, $\alpha^\tau = \tau\alpha$.

Il est bien évident que si N est décomposée sur $\varkappa$, W est proprement représenté. Il suffit de prendre un θ du lemme 5 et de poser $\alpha(\chi) = \langle \theta, \chi \rangle^{n_\chi}$.

Si réciproquement W est proprement représenté on cherchera à extraire un 2-cocycle convenable, c'est-à-dire un 2-cocycle μ qui engendre $\mathfrak{H}$ et qui vérifie $\mu^\tau = \tau\mu$ et $\mu(\chi, \chi')^n = \frac{\alpha(\chi)^{f_\chi}\alpha(\chi')^{f_{\chi'}}}{\alpha(\chi\chi')^{f_{\chi\chi'}}}$, si c'est possible l'extension $k(\sqrt[n]{\mathrm{E}^n}) = \mathrm{N}$ sera décomposée sur $\varkappa$.

Dans le cas particulier suivant c'est facile :

COROLLAIRE. — *Si $\tilde{k}$ ne contient que* 1 *comme racine $n^{\text{ième}}$ de l'unité, si α représente proprement* W *et vérifie pour tout couple χ, χ' :*

$$\frac{\alpha(\chi)^{f_\chi}\alpha(\chi')^{f_{\chi'}}}{\alpha(\chi\chi')^{f_{\chi\chi'}}} \in \tilde{k}^{*n}$$

alors l'extension associée à W *est décomposée.*

On posera $\mu(\chi, \chi')$ racine $n^{\text{ième}}$ dans $\tilde{k}$ de $\frac{\alpha(\chi)^{f_\chi}\alpha(\chi')^{f_{\chi'}}}{\alpha(\chi\chi')^{f_{\chi\chi'}}}$ et on vérifie facilement que μ est un 2-cocycle qui engendre $\mathfrak{H}$ et qui satisfait à $\mu^\tau = \tau.\mu$.

Nous pouvons noter que si la caractérisation des extensions décomposées sur $\varkappa$ n'est pas donnée sur le groupe W (resp. E^n), ce qui serait plus maniable pour les questions d'existence, mais sur un 2-cocycle convenable; la détermination de celui-ci n'exige pas de sortir de k^*. On peut même remarquer que si $\mathrm{N}/\varkappa$ est décomposée E^n et $\mathfrak{H}$ sont « définissables dans $\tilde{k}$ ». En effet si θ est un élément de K satisfaisant au lemme 5 on voit facilement que $\mu_\theta \in \bar{\mathbf{Z}}^2(\mathrm{X}, \tilde{k}^*)$.

En plus de son utilité vraisemblable pour l'étude des extensions abéliennes d'un corps ne contenant pas les bonnes racines de l'unité, la méthode donne des résultats appréciables dans l'étude de l'existence et des propriétés arithmétiques des extensions K à groupe de Galois isomorphe au groupe du carré ou au groupe des quaternions d'un corps $\varkappa$ de caractéristique différente de 2. Ces résultats ont été obtenus en collaboration avec Pierre Damey et seront publiés ultérieurement.

BIBLIOGRAPHIE.

[1] N. BOURBAKI, *Algèbre*, chap. V : *Corps commutatifs.*

[2] A. FRÖHLICH, *The module structure of Kummer extensions over Dedekind domains* (*J. reine angew. Math.*, vol. 209, nos 1-2, 1962, p. 39 à 53).

[3] M. HALL, *The theory of groups*, Mac Millan, New York, 1959.

[4] H. HASSE, *Invariante Kennzeichnung relativ abelschen Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers* (*Abh. der D. A. W. Akad-Verlag*, Berlin, 1947-1948).

[5] H. HASSE, *Invariante Kennzeichnung galoischer Körper mit vorgegebene Galoisgruppe* (*J. für Math.*, vol. 187).

[6] H. HASSE, *Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers* (*Math. Nach.*, 1948, p. 40 à 61, 213 à 217 et 277 à 283).

[7] J. MARTINET, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p* (*Thèse*, à paraître).

[8] J. MARTINET et J.-J. PAYAN, *Sur les extensions cubiques non galoisiennes des rationnels et leur clôture galoisienne* (*J. reine angew. Math.*, vol. 228, 1967, p. 15 à 37).

[9] J. MARTINET et J.-J. PAYAN, *Sur les bases d'entiers des extensions galoisiennes et non abéliennes de degré 6 des rationnels* (*J. reine angew. Math.*) (à paraître).

[10] J.-P. SERRE, *Applications algébriques de la cohomologie des groupes* (*Séminaire Henri Cartan*, 1950-1951, exp. 5).

(Manuscrit reçu le 19 novembre 1967.)