

L. BOUVIER

J. J. PAYAN

Construction de certaines extensions de degré p

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 75-84

http://www.numdam.org/item?id=STNG_1971-1972__1__75_0

© Institut Fourier – Université de Grenoble, 1971-1972, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

CONSTRUCTION DE CERTAINES EXTENSIONS DE DEGRE p

Exposé par L. BOUVIER le 19.4.72 d'après un travail avec J.J. PAYAN

INTRODUCTION.

Soient p un nombre premier impair et κ un corps de caractéristique différente de p . On se propose de construire les extensions K de degré p sur κ dont la clôture galoisienne N vérifie la condition suivante : le p -groupe de Sylow de $\text{Gal } N/\kappa$ est distingué. Cela revient à dire qu'il existe une extension intermédiaire k de N/κ vérifiant $\text{Gal } N/k \simeq \mathbb{Z}/p\mathbb{Z}$, k/κ cyclique de degré diviseur de $p-1$ et $\text{Gal } k/\kappa$ opère fidèlement sur $\text{Gal } N/k$.

Nous nous proposons de décrire, via la théorie de Kummer, la construction de ces extensions. Nous expliciterons au chap. III les énoncés dans les cas déjà étudiés ([3], [5], [2]) où k/κ est soit triviale, soit de degré premier q . L'utilisation de la décomposition en facteurs directs simples de l'algèbre $F_p[g']$ d'un groupe abélien fini g' d'exposant diviseur de $p-1$, nous permettra de clarifier un peu une question qui semble en avoir besoin...

I. ADJONCTION DES RACINES p -IÈMES DE L'UNITE.

Soit k une extension de κ , cyclique de degré q diviseur de $p-1$. Pour toute extension L de κ , nous noterons L' l'extension obtenue en adjoignant les racines p -ièmes de l'unité. On pose $g = \text{Gal } k/\kappa$ et $g' = \text{Gal } k'/\kappa$. Désignons par A la p -extension abélienne à groupe de Galois d'exposant p maximale, c'est-à-dire la composée de toutes les extensions cycliques de degré p sur k' . Il est clair que A/κ est galoisienne. Posons $G = \text{Gal } A/\kappa$, G est

un $\mathbb{F}_p[g']$ -module. Soit $X' = \text{Hom}(g', \mathbb{F}_p^*)$ et posons pour tout χ de X'

$$1_\chi = \frac{1}{[g':1]} \sum_{\tau \in g'} \chi(\tau^{-1}) \tau .$$

Comme l'exposant de g' divise $p-1$, on obtient ainsi un système complet d'idempotents primitifs et orthogonaux (cf [3]) grâce auxquels on peut écrire :

$$\mathbb{F}_p[g'] = \bigoplus_{\chi \in X'} \mathbb{F}_p[g'] 1_\chi .$$

Le $\mathbb{F}_p[g']$ -module G se décompose alors sous la forme $G = \bigoplus_{\chi \in X'} G_\chi$ où $G_\chi = G 1_\chi$.

Propriétés caractéristiques des éléments de G_χ , $\chi \in X'$.

Soit $\sigma \in G_\chi$, les assertions suivantes sont équivalentes :

- i) $\sigma \in G_\chi$
- ii) $\sigma = \sigma 1_\chi$
- iii) $\sigma^\tau = \sigma^{\chi(\tau)}$ pour tout $\tau \in g'$.

Les assertions i) et ii) sont trivialement équivalentes. Pour voir qu'il en est de même pour ii) et iii) il suffit de remarquer que $\tau.1_\chi = \chi(\tau)1_\chi$, quel que soit $\tau \in g'$.

Il est clair que les groupes G_χ sont fermés dans G pour la topologie de Krull. Pour $\chi \in X'$, on note A_χ l'extension intermédiaire de A/k' qui appartient à $\bigoplus_{\substack{\chi \in X' \\ \chi' \neq \chi}} G_{\chi'}$, ce sous-groupe étant distingué dans G , A_χ/κ est galoisienne. De plus, l'opération de g' sur $\text{Gal } A_\chi/\kappa$ est définie par :

$$\sigma \in \text{Gal } A_\chi/\kappa, \quad \tau \in g', \quad \sigma^\tau = \sigma^{\chi(\tau)} .$$

On peut alors énoncer :

Propriété.

Soit $\chi \in X'$ et soit N' une extension intermédiaire de A_χ/k' telle que N'/k' soit cyclique de degré p , alors N' est galoisienne sur κ et abélienne sur k_χ où k_χ désigne l'extension intermédiaire de k'/κ qui appartient au groupe $g'_\chi = \{\tau \in g' : \chi(\tau) = 1\}$. De plus k_χ est l'extension intermédiaire minimale de k'/κ sur laquelle N' est abélienne.

Nous allons maintenant déterminer les extensions N' cycliques de degré p sur k' qui contiennent une extension N du type cherché.

Proposition I.

Soit N' une extension cyclique de degré p sur k' . Pour qu'il existe N galoisienne sur κ , cyclique de degré p sur k telle que $N' = Nk'$, il faut et il suffit que N' soit une extension intermédiaire de l'une des extensions A_χ/k' où χ élément de X' est trivial sur $\text{Gal } k'/k$. De plus l'extension N correspondant à N' est unique et l'opération de g sur $\text{Gal } N/k$ est définie par :

$$\tau \in g, \sigma \in \text{Gal } N/k, \sigma^\tau = \sigma^{\chi(\tau)}$$

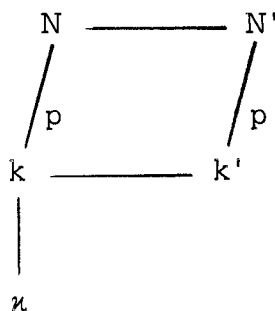
où χ est l'élément de X' tel que $N' \subset A_\chi$ (χ peut être considéré comme un caractère de g car il est trivial sur $\text{Gal } k'/k$).

Démonstration :

1. Soit N une extension cyclique de degré p sur k , galoisienne sur κ . Le groupe g opère sur $\text{Gal } N/k$; or $\text{Gal } N/k$ peut être considéré comme un espace vectoriel de dimension 1 sur \mathbb{F}_p , on a donc ainsi une représentation de dimension 1 de g sur \mathbb{F}_p , en désignant par χ le caractère de cette représentation, $\chi \in \text{Hom}(g, \mathbb{F}_p^*)$, l'opération de g sur $\text{Gal } N/k$ est définie par :

$$\sigma \in \text{Gal } N/k, \tau \in g, \sigma^\tau = \sigma^{\chi(\tau)}.$$

On peut prolonger χ pour en faire un caractère de g' à valeurs dans \mathbb{F}_p^* en posant $\chi(\tau) = 1$ pour tout $\tau \in \text{Gal}(k'/k)$, on désigne encore par χ l'élément de X' ainsi obtenu. Posons $N' = Nk'$, N' est galoisienne sur κ , cyclique de degré p sur k' et abélienne sur k .



On montre alors que l'opération de g' sur $\text{Gal } N'/k'$ est définie par :

$\sigma^\tau = \sigma^{\chi(\tau)}$ pour tout $\tau \in g'$ et tout $\sigma \in \text{Gal } N'/k'$. Il en résulte $N \subset A_\chi$.

2. Inversement, soit N' une extension cyclique de degré p sur k' telle que $N' \subset A_\chi$ où χ est un élément de X' trivial sur $\text{Gal } k'/k$, alors N' est galoisienne sur κ et abélienne sur k . Comme $(p, [k':k]) = 1$, N' se décompose sur k et il existe une extension N et une seule cyclique de degré p sur k , galoisienne sur κ .

Remarquons que si l'on considère $\chi \in X'$ trivial sur $\text{Gal } k'/k$ mais tel que $g'_\chi \neq \text{Gal } k'/k$, à une extension $N' \subset A_\chi$, cyclique de degré p sur k' correspond une extension N cyclique de degré p sur k , galoisienne sur κ et abélienne sur k_χ . Comme k_χ diffère de k , g n'opère pas fidèlement sur $\text{Gal } N/k$.

Par conséquent, les éléments de X' auxquels nous nous intéresserons, seront les caractères χ tels que $g'_\chi = \text{Gal } k'/k$, c'est-à-dire, en considérant χ comme un caractère de g , tels que si $\chi(\tau) = 1$ avec $\tau \in g$, alors $\tau = 1$.

Le corps k étant choisi, nous obtiendrons les extensions N et, par suite les extensions K , en construisant les extensions N' . De plus, nous allons regrouper les extensions N suivant la façon dont g opère sur $\text{Gal } N/k$, c'est-à-dire suivant le caractère χ de g à valeurs dans \mathbb{F}_p^* choisi.

Exemple : Prenons $p = 7$, $\kappa = \mathbb{Q}$ et $q = 3$. Au caractère trivial de g' correspondent les extensions N cycliques de degré 7 sur k , abéliennes sur κ ; aux deux autres caractères de g' triviaux sur $\text{Gal } k'/k$ sont associées deux familles d'extensions N cycliques de degré p sur k , galoisiennes et non abéliennes sur \mathbb{Q} . Le groupe de Galois des premières (resp. secondes) est défini par les générateurs σ , τ et les relations $\sigma^7 = 1$, $\tau^3 = 1$ et $\tau\sigma\tau^{-1} = \sigma^2$ (resp $\tau\sigma\tau^{-1} = \sigma^4$). Ces deux groupes de Galois sont d'ailleurs isomorphes.

II. LE CORPS $k_{\tilde{\chi}}$.

Soit χ un élément de X' trivial sur $\text{Gal } k'/k$ fixé.

Désignons par $F'_{\tilde{\chi}}$ le sous-groupe des éléments α de k'^* tels que $\alpha = \theta^p$ avec $\theta \in A_{\chi}$. L'ensemble des éléments α de k'^* tels que $N' = k'(\alpha^{1/p})$ soit cyclique de degré p sur k' et contenue dans A_{χ} est $F'_{\tilde{\chi}} \setminus k'^{*p}$. Ce paragraphe est consacré à déterminer $F'_{\tilde{\chi}}$.

En utilisant la théorie de Kummer -cf [1] et [6]- pour A_{χ} , on obtient la suite exacte :

$$1 \rightarrow k'^{*p} \rightarrow F'_{\tilde{\chi}} \xrightarrow{u} \text{Hom}_{\text{cont}}(G_{\chi}, k'^*) \rightarrow 1$$

où u est l'homomorphisme qui à $\alpha = \theta^p$ $\theta \in A_{\chi}$, fait correspondre le caractère : $\sigma \rightarrow \theta^{1-\sigma}$, $\sigma \in G_{\chi}$. On note \bar{u} l'isomorphisme de $F'_{\tilde{\chi}}/k'^{*p}$ sur $\text{Hom}_{\text{cont}}(G_{\chi}, k'^*)$ obtenu à partir de u par passage au quotient.

On peut remarquer que g' opère par Galois sur $F'_{\tilde{\chi}}/k'^{*p}$: en effet, k'^{*p} est globalement invariant par g' et pour tout $\alpha \in F'_{\tilde{\chi}}$ et tout $\tau \in g'$, $\alpha^{\tau} \in F'_{\tilde{\chi}}$. On en déduit une opération Φ' de g' sur $\text{Hom}_{\text{cont}}(G_{\chi}, k'^*)$ telle que l'action de g' commute avec \bar{u} . Et on montre que, pour tout $\psi \in \text{Hom}_{\text{cont}}(G_{\chi}, k'^*)$ et tout $\tau \in g'$,

$$\Phi'(\tau)\psi = \psi^{\tilde{\chi}(\tau)} \text{ avec } \tilde{\chi} = \chi^{-1}\chi_*$$

Le caractère χ_* -noté χ^* dans [4]- désigne l'élément de X' défini par $\zeta^{\tau} = \zeta^{\chi_*(\tau)}$ pour tout τ de g' (ζ racine primitive p -ième de l'unité). Le sous-groupe g'_{χ_*} de g' sur lequel χ_* est trivial, est $\text{Gal } k'/k'$.

Remarquons que $\ker \Phi' = g'_{\tilde{\chi}}$ -cf [6]-.

Par définition même de Φ' , il est clair que si $\alpha \in F'_{\tilde{\chi}}$, $\alpha^{\tau} = \alpha^{\tilde{\chi}(\tau)}$ dans k' , pour tout $\tau \in g'$ ($a =_p b$ dans k' signifiant que $a = bc^p$ avec $c \in k'$). Cette propriété est caractéristique des éléments de $F'_{\tilde{\chi}}$ en effet si $\alpha^{\tau} = \alpha^{\tilde{\chi}(\tau)}$ pour tout $\tau \in g'$, l'extension $N' = k'(\alpha^{1/p})$ est contenue dans A_{χ} . D'où la proposition suivante :

Proposition II.1.

$F'_{\tilde{\chi}}$ est l'ensemble des éléments α de k'^* tels que pour tout $\tau \in g'$,

$$\alpha^\tau \underset{p}{=} \alpha^{\tilde{\chi}(\tau)} \text{ dans } k' .$$

Or on montre :

Lemme.

Le sous-groupe $g'_{\tilde{\chi}}$ de g' est cyclique.

Remarquons d'abord que $g'_{\chi} \cap g'_{\chi_*} = \{1\}$, cela entraîne $g'_{\tilde{\chi}} \cap g'_{\chi} = \{1\}$ et la restriction à $g'_{\tilde{\chi}}$ de l'homomorphisme canonique de g' sur le groupe cyclique g'/g'_{χ} est injective.

Désignons par $k_{\tilde{\chi}}$ l'extension intermédiaire de k'/\mathfrak{u} qui appartient à $g'_{\tilde{\chi}}$. On peut remarquer que $k_{\tilde{\chi}}/\mathfrak{u}$ est cyclique.

Si k' et $k_{\tilde{\chi}}$ sont distincts, $k_{\tilde{\chi}}$ ne contient pas de racines p -ièmes de 1 autre que 1 car $g'_{\tilde{\chi}} \cap g'_{\chi_*} = \{1\}$. A l'aide de la proposition II.1 et du théorème 90 de Hilbert on démontre alors la propriété suivante (triviale lorsque $k_{\tilde{\chi}} = k'$).

Propriété II.2.

$F'_{\tilde{\chi}}$ est définissable dans $k_{\tilde{\chi}}$.

C'est-à-dire que quel que soit $\alpha \in F'_{\tilde{\chi}}$, il existe $\beta \in k_{\tilde{\chi}}$ tel que $\alpha \underset{p}{=} \beta$ dans k' . Notons $F_{\tilde{\chi}} = F'_{\tilde{\chi}} \cap k_{\tilde{\chi}}$, $F_{\tilde{\chi}} \supset k_{\tilde{\chi}}^{*p}$ et $F_{\tilde{\chi}}/k_{\tilde{\chi}}^{*p}$ est isomorphe à $F'_{\tilde{\chi}}/k'^{*p}$. Quelle que soit l'extension N' cyclique de degré p sur k' et contenue dans A_{χ} , il existe $\alpha \in F_{\tilde{\chi}}$ tel que $N' = k'(\alpha^{1/p})$.

En corollaire des deux propositions précédentes, on obtient :

Propriété II.3.

$F_{\tilde{\chi}}$ est l'ensemble des éléments α de $k_{\tilde{\chi}}^*$ tels que $\alpha^\tau \underset{p}{=} \alpha^{\tilde{\chi}(\tau)}$ dans
 $k_{\tilde{\chi}}$ pour tout $\tau \in \text{Gal } k_{\tilde{\chi}}/\mathfrak{u}$.

(en considérant $\tilde{\chi}$ comme un caractère de $\text{Gal } k_{\tilde{\chi}}/\mathfrak{u}$)

Or $\mathfrak{u} = k_{\tilde{\chi}}^*/k_{\tilde{\chi}}^{*p}$ est un $\mathbb{F}_p[\text{Gal } k_{\tilde{\chi}}/\mathfrak{u}]$ -module qui se décompose sous la forme -cf [4]- :

$$\mathfrak{U} = \bigoplus_{\varphi \in \text{Hom}(\text{Gal } k_{\tilde{\chi}}/\kappa, \mathbb{F}_p^*)} \mathfrak{U}_{\varphi}$$

où $\mathfrak{U}_{\varphi} = \mathfrak{U}^{1_{\varphi}}$ et $1_{\varphi} = \frac{1}{[\text{Gal } k_{\tilde{\chi}}/\kappa:1]} \sum_{\tau \in \text{Gal } k_{\tilde{\chi}}/\kappa} \varphi(\tau^{-1})\tau$. Et une propriété caractéristique des éléments a de \mathfrak{U}_{φ} est que $a^{\tau} = a^{\varphi(\tau)}$ pour tout $\tau \in \text{Gal } k_{\tilde{\chi}}/\kappa$, alors

Théorème 1.

$$F_{\tilde{\chi}} = \mathfrak{U}_{\tilde{\chi}} k_{\tilde{\chi}}^{*p}$$

On obtient ainsi une méthode simple et explicite pour construire une extension N' cyclique de degré p sur k' , contenue dans $A_{\tilde{\chi}}$; il suffit de prendre $N' = k'(\alpha^{1/p})$ où $\alpha = \beta^{1_{\tilde{\chi}}}$ avec $\beta \in k_{\tilde{\chi}}^*$ et

$$1_{\tilde{\chi}} = \frac{1}{[\text{Gal } k_{\tilde{\chi}}/\kappa:1]} \sum_{\tau \in \text{Gal } k_{\tilde{\chi}}/\kappa} \tilde{\chi}(\tau^{-1})\tau$$

en choisissant β pour que $\alpha \in k_{\tilde{\chi}} \setminus k_{\tilde{\chi}}^p$.

III. CAS OÙ k/κ N'ADMET PAS D'EXTENSION INTERMEDIAIRE NON TRIVIALE.

Le degré $[k:\kappa]$ est alors égal à 1 ou à un nombre premier q .

Posons $n = [\kappa':\kappa]$.

1. Cas où $[k:\kappa] = 1$.

Alors K est abélienne de degré p sur κ (pour $\kappa = \mathbb{Q}$, cf. [3]). On retrouve ainsi la construction des extensions abéliennes de degré p sur κ' , galoisiennes sur κ .

2. Cas où $[k:\kappa] = 2$.

On retrouve alors la construction des extensions diédrales exposée dans [5].

Le seul caractère χ à considérer est le caractère non trivial de g . On démontre le théorème :

Théorème 2.

Pour $[k:\kappa] = 2$,

A - Cas où k et κ' sont linéairement disjoints, alors $k_{\tilde{\chi}}$ est l'extension intermédiaire qui appartient au sous-groupe $\{1, S^{n/2} \tau\}$ de g' où S (resp τ) est un générateur de $\text{Gal } k'/k$ (resp $\text{Gal } k'/\kappa'$), et, $[k_{\tilde{\chi}}:\kappa] = n$.

B - Cas où $k \subset \kappa'$:

B_1 : si $k \neq \kappa'$ et $n \equiv 0 \pmod{4}$, alors $k_{\tilde{\chi}} = \kappa'$.

B_2 : si $k \neq \kappa'$ et $n \not\equiv 0 \pmod{4}$, alors $k_{\tilde{\chi}}$ est l'extension intermédiaire réelle maximale de κ'/κ .

B_3 : si $k = \kappa'$ alors $\chi = \chi_0$ et $k_{\tilde{\chi}} = \kappa$.

3. Cas où $[k:\kappa] = q$ premier impair.

On obtient alors la construction des extensions galoisiennes et non abéliennes de degré pq évoquée dans [2].

On a déjà vu que $p \equiv 1 \pmod{q}$.

Les caractères χ que nous considèrerons sont les $q-1$ caractères non triviaux de g .

A - Cas où k et κ' sont linéairement disjoints : g' est alors isomorphe au produit direct de g engendré par τ et de $\text{Gal } \kappa'/\kappa$ engendré par s .

Si $n \not\equiv 0 \pmod{q}$, alors $k_{\tilde{\chi}} = \kappa'$.

Si $n \equiv 0 \pmod{q}$, on montre que $g_{\tilde{\chi}}$ est engendré par τs^{n_0} où $n_0 \in \{1, 2, \dots, q-1\}$ est défini par $\chi(\tau) = \chi_*^{n_0}(s)$. On remarque que si χ_1 et χ_2 sont deux caractères non triviaux distincts de g , $k_{\tilde{\chi}_1}$ et $k_{\tilde{\chi}_2}$ sont distincts. Il y a donc alors $q-1$ corps $k_{\tilde{\chi}}$ associés au corps k .

B - Cas où $k \subset \kappa'$: Dans le cas simple où $k = \kappa'$, $\chi = \chi_*^t$ avec

$t \in \{1, 2, \dots, q-1\}$. Pour $t \neq 1$, $k_{\tilde{\chi}} = \kappa'$ et pour $t = 1$, $k_{\tilde{\chi}} = \kappa$.

Si $k \neq \kappa'$, on obtient un résultat analogue au cas où $[k:\kappa] = 2$.

- si $n \equiv 0 \pmod{q^2}$, $k_{\tilde{\chi}} = \kappa'$.

- si $n \not\equiv 0 \pmod{q^2}$, il existe un caractère non trivial χ de g et un

seul tel que $k_{\tilde{\chi}} \neq \kappa'$, à savoir $\chi = \chi_*^{m/q}$ avec $m \in \{1, 2, \dots, \frac{n}{q}\}$ et $(1 - m \frac{n}{p}, q) \neq 1$; $k_{\tilde{\chi}}$ est alors l'extension intermédiaire de κ'/κ de degré $\frac{n}{q}$ sur κ .

En résumé :

Théorème 3.

Pour $[k:\kappa] = q$ premier impair,

A - Cas où k et κ' sont linéairement disjoints :

A_1 : si $n \not\equiv 0 \pmod{q}$, $k_{\tilde{\chi}} = \kappa'$.

A_2 : si $n \equiv 0 \pmod{q}$, $[k_{\tilde{\chi}}:\kappa] = n$ et pour $\chi_1 \neq \chi_2$, $k_{\tilde{\chi}_1} \neq k_{\tilde{\chi}_2}$.

B - Cas où $k \subset \kappa'$:

B_1 : si $k \neq \kappa'$ et $n \equiv 0 \pmod{q^2}$, $k_{\tilde{\chi}} = \kappa'$

B_2 : si $k \neq \kappa'$ et $n \not\equiv 0 \pmod{q^2}$, il existe un caractère χ non trivial unique de g tel que $k_{\tilde{\chi}} \neq \kappa'$

B_3 : si $k = \kappa'$, $k_{\tilde{\chi}} = \kappa'$ si $\chi \neq \chi_*$
 $k_{\tilde{\chi}} = \kappa$ si $\chi = \chi_*$.

Remarque : On retrouve des résultats bien connus d'obstruction locale au problème du plongement dans le cas décomposé. C'est ainsi que si κ est une extension finie de $\mathbb{Q}_{p'}$, avec $p' \neq p$, $F_{\tilde{\chi}}$ est trivial. Il n'existe donc pas de plongement de l'extension k/κ cyclique de degré q donné dans une extension galoisienne et non abélienne de degré pq sur κ .

Dans le cas de caractéristique résiduelle égale à p , l'étude du groupe V_k , des unités distinguées de k' , comme $\mathbb{Z}_p[g']$ -module permet sans doute de distinguer les χ pour lesquels $F_{\tilde{\chi}}$ est non trivial.

BIBLIOGRAPHIE

- [1] - CASSELS et FRÖLICH - "Algebraic Number Theory".
New York 1967.
- [2] - J. COUGNARD - "Sur les extensions galoisiennes non abéliennes
de degré pq (p et q premiers) des rationnels"
Note au C.R.A.S. 274 A (1972) pp. 936-939.
- [3] - G. GRAS - "Sur le ℓ -groupe des classes des extensions
cycliques de degré ℓ de \mathbb{Q} ".
Sém. Th. Nombres. Grenoble - Janv. 72.
- [4] - H. W. LEOPOLDT - "Zur Struktur der ℓ -Klassengruppe galoischer
Zahlkörper".
Journ. für d. reine u. angew. Math. 199, (1958)
pp. 165-174.
- [5] - J. MARTINET - "Sur l'arithmétique des extensions galoisiennes
à groupe de Galois diédral d'ordre $2p$ ".
Thèse 1968.
- [6] - J.J. PAYAN - "Critère de décomposition d'une extension de
Kummer".
Ann. Scient. de l'E.N.S. 4e série, t.1 (1968)
pp. 445-458.
-