Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Thong Nguyen-Quang-Do

Le plongement caloisien à noyau d'ordre premier et ses applications à la construction d'extensions non abéliennes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 17, n° 2 (1975-1976), exp. n° G5, p. G1-G5

<http://www.numdam.org/item?id=SDPP_1975-1976__17_2_A11_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'Etude de théorie des nombres)
17e année, 1975/76, n° G5, 5 p.

10 novembre 1975

LE PLONGEMENT GALOISIEN À NOYAU D'ORDRE PREMIER ET SES APPLICATIONS À LA CONSTRUCTION D'EXTENSIONS NON ABÉLIENNES

par NGUYEN-QUANG-DO Thong

Introduction.

Etant donné un corps arithmétique k (i. e. un corps local ou global), le grand problème est : Pour tout groupe G, classifier les extensions galoisiennes de k dont le groupe de Galois est isomorphe à G. Si G est abélien, le problème est résolu par la théorie du corps de classes. Il n'y a pas encore de théorie satisfaisante dans le cas non abélien. Si G n'est pas abélien, on peut se limiter au cas où G est résoluble, et faire des constructions par induction : c'est le problème inverse de la théorie de Galois. Plus précisément :

Soit K/k galoisienne, de groupe G. Soit l'extension de groupe :

$$(E) \qquad 1 \longrightarrow A \xrightarrow{i} E \xrightarrow{s} G \longrightarrow 1 .$$

Construire une extension $L/(K/k)$ telle que L/K soit galoisienne de groupe A, et L/k galoisienne de groupe E, et telle que le passage au quotient s corresponde sur les groupes de Galois à la restriction des automorphismes de L à K. Ce problème est appelé problème du plongement relatif à K/k et la suite exacte (E) ; A est le noyau du plongement.

Nous nous occuperons ici d'un plongement particulier :

Soit k un corps $\mathfrak{L}$-adique, i. e. une extension finie d'un corps $\mathbb{Q}_\ell$ de nombres ℓ-adiques. Soit p un nombre premier. Etant donnée une extension galoisienne K/k, de groupe G, trouver toutes les extensions L qui sont cycliques de degré p sur K et galoisiennes sur k.

Nous appellerons $(K/k\ ,\ p)$ ce problème. Le nombre des solutions est noté $N(K/k\ ,\ p)$. On a $N(K/k\ ,\ p) < \infty$ d'après un résultat de KRASNER [3] sur la finitude du nombre des extensions de degré donné d'un corps $\mathfrak{L}$-adique. Nous allons calculer $N(K/k\ ,\ p)$, et appliquer les résultats à la détermination des extensions galoisiennes de k dont le groupe est non abélien, pas trop compliqué.

1. Résultats géométriques.

Définitions. - Pour toute extension K de $\mathbb{Q}_\ell$, de degré n, et pour tout nombre premier p, soit Γ_K le groupe K^*/K^{*p}, considéré comme espace vectoriel sur $\mathbb{F}_p$. Alors $\dim \Gamma_K = \alpha n + 1 + \varepsilon$, avec $\alpha = 1$ (resp. 0) si $p = \ell$ (resp. $p \neq \ell$) et $\varepsilon = 1$ (resp. 0) si K contient (resp. ne contient pas) le groupe A_p des racines p-ièmes de l'unité (cf. par exemple CASSELS-FRÖHLICH [1]).

THÉORÈME 1.1. - Pour toute extension galoisienne K/k, de groupe G, et pour tout nombre premier p, le nombre $N(K/k, p)$ est égal :

(i) au nombre des hyperplans de Γ_K stables par G,

(ii) au nombre des droites de l'espace dual $\hat{\Gamma}_K$ stables par G.

Preuve. - Par le corps de classes [1] ou par la théorie de Galois, on obtient des conditions nécessaires et suffisantes pour qu'une extension L/K, cyclique de degré p, soit galoisienne sur k. La traduction en langage géométrique donne le théorème.

C. Q. F. D.

Si K contient le groupe A_p des racines p-ièmes de l'unité, le symbole de puissance p-ième [1] permet de définir, par passage au quotient, une forme bilinéaire antisymétrique, non dégénérée, notée $\langle . , . \rangle_K$. Par rapport à cette forme, le groupe $G = \mathrm{Gal}(K/k)$ agit comme un groupe de similitudes. Plus précisément, $\forall\, \sigma \in G$, $\forall\, \alpha \in \Gamma_K$, $\forall\, \beta \in \Gamma_K$, $\langle \sigma\alpha , \sigma\beta \rangle = j\langle \alpha , \beta \rangle$, où $j = j(\sigma)$ est l'élément de $\underset{\sim}{F}_p$ défini par $\sigma(\zeta) = \zeta^j$, ζ générateur de A_p. On peut alors compléter 1.1.

THÉORÈME 1.1 bis. - Dans les hypothèses de 1.1, supposons, en plus, que K contient A_p. Alors $N(K/k , p)$ = nombre des droites de Γ_K laissées stables par G.

Preuve. - En effet, toute similitude conservant l'orthogonalité, il y aura bijection entre les hyperplans stables par G et les droites (orthogonales à ces hyperplans) stables par G.

C. Q. F. D.

2. Cas où $\mathrm{Gal}(K/k)$ est un p-groupe.

Définitions. - Pour tout p-groupe G, on notera $I_G = I$ l'idéal d'augmentation de l'algèbre de groupe $\underset{\sim}{F}_p[G]$, i. e. la sous-algèbre engendrée par $(\sigma - 1)$, $\sigma \in G$.

PROPOSITION 2.1. - Si $G = \mathrm{Gal}(K/k)$ est un p-groupe, $N(K/k , p)$ est égal au nombre de sous-groupes d'ordre p du groupe d'homologie $H_0(G , \Gamma_K) = \Gamma_K / I\Gamma_K$.

Preuve. - Si G est un p-groupe, les valeurs propres de tout σ G sont égales à 1. Donc $N(K/k , p)$ = nombre des vecteurs de $\hat{\Gamma}_K$ fixes par G, d'où le résultat, par dualité.

C. Q. F. D.

PROPOSITION 2.1 bis. - Si, en plus, K contient A_p , $N(K/k , p)$ est égal au nombre des sous-groupes d'ordre p du groupe de cohomologie $H^0(G , \Gamma_K) = \Gamma_K^G$.

On peut toujours, par extension du corps k (et moyennant quelques précautions !), supposer que k contient A_p . Alors, si $\dim \Gamma_K^G = C$, on aura :

$$N(K/k , p) = (p^c - 1)/(p - 1)$$

d'après 2.1 bis. Il reste à calculer c .

THÉORÈME 2.2. - Soit k un corps ℓ-adique contenant A_p . Soit K/k galoisienne de groupe G (G = un p-groupe). Alors $\dim \Gamma_K^G = \alpha n + 2 - \beta + r - d$, où :

$n = [k : \mathbb{Q}_\ell]$,

$\alpha = 1$ (resp. 0) si p divise ℓ (resp. ne divise pas) ,

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

r = nombre minimal de relations de G = $\dim H^2(G , A_p)$,

$\beta = 0$ (resp. 1) si l'image de $H^2(G , A_p)$ dans $H^2(G , K^*)$ est 0 (resp. $\neq 0$) .

Preuve. - Des deux suites exactes

$$1 \longrightarrow K^{*p} \longrightarrow K^* \longrightarrow \Gamma_K \longrightarrow 1 \quad \text{et} \quad 1 \longrightarrow A_p \longrightarrow K^* \longrightarrow K^{*p} \longrightarrow 1 ,$$

on tire les suites exactes de cohomologie :

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

et

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

La première donne $\Gamma_K^G / \mathrm{Im}\ \eta \simeq H^1(G , K^{*p})$, où η est l'homomorphisme canonique de Γ_k dans Γ_K , et par KUMMER, on sait que $\mathrm{Ker}\ \eta \simeq H^1(G , A_p)$.

La seconde suite montre que $H^1(G , K^{*p})$ s'injecte dans $H^2(G , A_p)$ par ψ , avec $\mathrm{Coker}\ \psi \simeq \mathrm{Im}\ \varphi$. Or, d'après le corps de classes [1], $H^2(G , K^*)$ est cyclique, et comme $H^2(G , A_p)$ est d'exposant p , $\mathrm{Im}\ \varphi$ est au plus d'ordre p .

C. Q. F. D.

3. Cas où Gal(K/k) est d'ordre premier à p .

On suppose que k est une extension finie de $\mathbb{Q}_p$, contenant A_p Si K/k est galoisienne de groupe G , d'ordre premier à p , l'algèbre $\mathbb{F}_p[G]$ est semi-simple et l'extension K/k est modérément ramifiée.

Définitions. - Soit v_K la valuation de K . Pour tout entier $m \geq 0$, on pose :

$U_K^0 = U_K$ = groupe des unités de K ,

$U_K^m = \{x \in K^* ; \ v(1 - x) \geq m\}$ pour $m \geq 1$,

$e_K = v(p)$ et $e'_K = v(p)/(p-1)$ ($= v(\zeta - 1)$, ζ générateur de A_p).

THÉORÈME 3.1. - Dans ces conditions,

$$N(K/k\ ,\ p) = \frac{p^{n+2} - 1}{p - 1} + t\,\frac{p^n - 1}{p - 1}\ ,$$

où $n = [k : \underset{\sim}{Q}_p]$ et $t = |\mathrm{Hom}(G\ ,\ \underset{\sim}{F}_p^*) - 1|$.

Preuve. - Le problème revient à compter la multiplicité avec laquelle une représentation de dimension 1 intervient dans l'espace de représentation Γ_K de G sur $\underset{\sim}{F}_p$. En posant $\Gamma_K^m = U_K^m K^{*p}/K^{*p}$ pour $m \geq 0$, on voit facilement que :

- l'espace de représentation Γ_K est somme directe de Γ_K^1 et d'un espace de dim 1 sur lequel G opére trivialement,
- G opère trivialement sur $\Gamma_K^{pe'_K}$.

Reste à étuiier l'action de G sur $\Gamma_K^1/\Gamma_K^{pe'_K}$. Pour cela, on le filtre par les $\Gamma_K^m/\Gamma_K^{pe'_K}$, et on utilise un résultat d'IWASAWA [2].

C. Q. F. D.

4. Extensions galoisiennes non abéliennes de certains types donnés.

Dans tout ce paragraphe, $[k : \underset{\sim}{Q}_p] = n$, k contient A_p . On va appliquer les résultats précedents à la détermination des extensions galoisiennes de k dont le groupe est isomorphe à un groupe non abélien donné, pas trop compliqué.

PROPOSITION 4.1. - Soit q premier, $\neq p$. Le nombre des extensions diédrales de k , de degré pq , est égal à $(q^2 - 1)(p^n - 1)/(p - 1)$ si q divise $p - 1$, 0 sinon.

Preuve. - On remarque que si L/k est une extension galoisienne de degré pq , $\mathrm{Gal}(L/k)$ admet un sous-groupe normal d'ordre p , et un seul, d'après la théorie de la ramification. Le reste s'ensuit aisément.

C. Q. F. D.

(4.2) : On veut déterminer les extensions non abéliennes de degré p^3 de k ($p \neq 2$, ou $p = 2$) . Les résultats sont trop compliqués pour être énoncés ici (voir [4]). La méthode consiste, étant donnée K/k galoisienne, de groupe G , de type $(p\ ,\ p)$, à déterminer Γ_K^G en "descendant" dans les sous-extensions de K . Le langage géométrique est essentiel pour la clarté des calculs.

(4.3) : Pour finir, donnons une application cohomologique :

PROPOSITION. - Soit G un p-groupe abélien dont le nombre minimal de générateurs (resp. de relations) est d (resp. r) . Alors $r = d(d + 1)/2$.

La preuve consiste à fabriquer une extension galoisienne K/k , de groupe G ,

telle que $H^2(G , A_p)$ s'identifie à $H^1(G , K^{*p})$. On utilise alors la suite exacte d'inflation-restriction (il faut une étude assez fine) pour déterminer le H^1 par "dévissage" de G . Il serait plaisant, par une méthode analogue, de redémontrer la célèbre (voir [1]) inégalité de Golod-Šafarevič, $r \geq d^2/4$.

Je n'y suis pas arrivé.

BIBLIOGRAPHIE

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

[2] IWASAWA (K.). - On Galois groups of local fields, Trans. Amer. math. Soc., t. 80, 1955, p. 448-469.

[3] KRASNER (M.). - Nombre des extensions d'un degré donné d'un corps p-adique, "Colloques internationaux du C. N. R. S., 143 : Les tendances géométriques en algèbre et théorème des nombres [1964. Clermont-Ferrand], p. 143-169. - Paris, Centre National de la Recherche Scientifique, 1966.

[4] MASSY (R.) et NGUYEN-QUANG-DO Thong. - 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 10 novembre 1975)

NGUYEN-QUANG-DO Thong
21 rue des Sablons
91350 GRIGNY