

IGOR R. ŠAFAREVIČ

Extensions à points de ramification donnés (résumé français)

Publications mathématiques de l'I.H.É.S., tome 18 (1963), p. 93-95

http://www.numdam.org/item?id=PMIHES_1963__18__93_0

© Publications mathématiques de l'I.H.É.S., 1963, tous droits réservés.

L'accès aux archives de la revue « Publications mathématiques de l'I.H.É.S. » (<http://www.ihes.fr/IHES/Publications/Publications.html>) 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/>

RÉSUMÉ DU MÉMOIRE PRÉCÉDENT

Soient k un corps de nombres algébriques, S un ensemble fini de places de k (archimédiennes ou non), et l un nombre premier. On note K_S la plus grande extension galoisienne de k dont le groupe de Galois \mathfrak{G}_S soit un pro- l -groupe (i.e. une limite projective de l -groupes finis), et qui soit non ramifiée en dehors de S .

[Rappelons que, si v est une place archimédienne, on dit que v est ramifiée si le degré de l'extension locale correspondante est égal à 2. Toute place complexe est non ramifiée; une place réelle est non ramifiée si et seulement si elle reste réelle (c'est toujours le cas si $l \neq 2$). Dans la suite, on supposera que les places archimédiennes contenues dans S sont toutes réelles.]

On se propose d'évaluer les deux entiers suivants :

$$d(\mathfrak{G}_S) = \text{nombre minimal de générateurs topologiques de } \mathfrak{G}_S \\ = \dim. H^1(\mathfrak{G}_S, \mathbf{Z}/l\mathbf{Z}) = \dim. \mathfrak{G}_S / (\mathfrak{G}_S, \mathfrak{G}_S) \cdot \mathfrak{G}_S^l,$$

$$r(\mathfrak{G}_S) = \text{nombre minimal de « relations » entre éléments d'un système minimal de} \\ \text{générateurs topologiques de } \mathfrak{G}_S \\ = \dim. H^2(\mathfrak{G}_S, \mathbf{Z}/l\mathbf{Z}).$$

[Toutes les dimensions sont relatives au corps $\mathbf{Z}/l\mathbf{Z}$.]

En fait, l'auteur détermine explicitement $d(\mathfrak{G}_S)$, et donne une *majoration* de $r(\mathfrak{G}_S) - d(\mathfrak{G}_S)$; l'intérêt principal du résultat est de montrer que $r(\mathfrak{G}_S) - d(\mathfrak{G}_S)$ est « petit »; modulo des théorèmes à démontrer sur les l -groupes, cela devrait entraîner le fait que \mathfrak{G}_S est *infini* (pour des choix convenables de k).

1. Calcul du nombre de générateurs.

La théorie du corps de classes permet d'identifier le groupe $\mathfrak{G}_S / (\mathfrak{G}_S, \mathfrak{G}_S) \cdot \mathfrak{G}_S^l$ au groupe $J/\mathfrak{U}_S J^l k^*$, où J désigne le groupe des idèles de k , et \mathfrak{U}_S le sous-groupe de J formé des idèles de la forme (x_v) , où x_v est une unité pour tout $v \notin S$, et $x_v = 1$ pour $v \in S$ [lorsque v est archimédienne, on convient que tout élément du corps local k_v est une unité].

La dimension du groupe $J/\mathfrak{U}_S J^l k^*$ se calcule au moyen d'un certain nombre de suites exactes. Le résultat est le suivant (cf. th. 1, p. 73) :

Théorème 1. — On a $d(\mathfrak{G}_S) = \dim(V_S/k^{*l}) + \sum_{v \in S} \dim(\mathfrak{U}_v/\mathfrak{U}_v^l) - r - \delta$, où :

$V_S = \mathfrak{U}_S J^l \cap k^* =$ ensemble des $x \in k^*$ qui sont des puissances l^e dans tous les k_v , $v \in S$, et dont les valuations relativement aux $v \notin S$ sont divisibles par l .

$r =$ rang rationnel du groupe des unités de k

$= r_1 + r_2 - 1$, avec les notations habituelles.

$\delta = \begin{cases} 1 & \text{si } k \text{ contient une racine primitive } l^e \text{ de l'unité} \\ 0 & \text{sinon.} \end{cases}$

Bien entendu, les $\dim(\mathcal{U}_v/\mathcal{U}_v^l)$ peuvent être explicitées. Cela permet de mettre $d(\mathfrak{G}_S)$ sous la forme suivante :

$$d(\mathfrak{G}_S) = t(S) + \lambda(S) + \sigma(S) - r - \delta,$$

avec :

$t(S)$ = nombre des $v \in S$ tels que k_v contienne une racine primitive l^e de l'unité.

$\sigma(S) = \dim(V_S/k^{*l})$.

$\lambda(S) = \sum n(v)$, pour $v \in S$ divisant l , où $n(v)$ est le degré du corps local k_v sur \mathbf{Q}_v .

2. Nombre de relations.

Posons $E(G) = H^2(G, \mathbf{Z}/l\mathbf{Z})$, groupe des classes d'extensions de G par $\mathbf{Z}/l\mathbf{Z}$. On doit évaluer $r(\mathfrak{G}_S) = \dim.E(\mathfrak{G}_S)$. Si l'on écrit le groupe $G = \mathfrak{G}_S$ sous la forme $\varprojlim G_\alpha$, où les G_α sont finis, et si l'on note $E(G_\alpha)^0$ le noyau de $E(G_\alpha) \rightarrow E(G)$, on a évidemment :

$$r(G) = \sup_\alpha \dim.E(G_\alpha)/E(G_\alpha)^0.$$

L'auteur interprète ces $E(G_\alpha)$ et $E(G_\alpha)^0$ en termes de « problèmes de plongement ». Voici ce qu'il entend par là : soit K_α le sous-corps de K_S ayant pour groupe de Galois sur k le groupe G_α . Soit d'autre part $e \in E(G_\alpha)$. Le « problème de plongement pour e » consiste à trouver une extension K_e de K_α , galoisienne sur k , cyclique de degré l sur K , et telle que le groupe de Galois de K_e/k soit l'extension de G_α par $\mathbf{Z}/l\mathbf{Z}$ correspondant à e . On dit que le problème de plongement est *résoluble dans* K_S si l'on peut choisir pour K_e un sous-corps de K_S . Ceci étant, il est facile de voir que $E(G_\alpha)^0$ est l'ensemble des $e \in E(G_\alpha)$ tels que le problème de plongement correspondant soit résoluble dans K_S (cf. th. 2, p. 78).

A côté de $E(G_\alpha)$, on introduit le sous-groupe $\widetilde{E(G_\alpha)}$ formé des éléments e pour lesquels le problème de plongement est résoluble (dans la clôture algébrique de k). On a tout d'abord (cf. th. 3, p. 79) :

$$\dim.E(G_\alpha)/\widetilde{E(G_\alpha)} \leq t(S) - \delta$$

(resp. $E(G) = \widetilde{E(G_\alpha)}$ si $S = \emptyset, \delta = 1$),

avec les notations du n° 1.

On définit d'autre part (cf. th. 4, p. 80) un plongement du groupe $E(G_\alpha)/\widetilde{E(G_\alpha)}^0$ dans $\text{Coker}(\hat{\varphi})$, où $\varphi : \mathfrak{A}_S \rightarrow J/k^*$ est l'application évidente, et $\hat{\varphi}$ sa transposée par rapport au foncteur $\text{Hom}(\quad, \mathbf{Z}/l\mathbf{Z})$. D'où l'inégalité :

$$\dim.\widetilde{E(G_\alpha)}/E(G_\alpha)^0 \leq \dim.\text{Ker}(\varphi_i),$$

où φ_i désigne l'application canonique de $\mathfrak{A}_S/\mathfrak{U}_S^l$ dans $J/J^l k^*$. En regroupant ces diverses inégalités, et en calculant la dimension de $\text{Ker}(\varphi_i)$, on obtient finalement :

Théorème 5. — Les notations étant celles du n° 1, on a :

$$r(\mathfrak{G}_S) \leq t(S) + \sigma(S) - \delta$$

(resp. $r(\mathfrak{G}_S) \leq \sigma(S)$ si $S = \emptyset, \delta = 1$).

3. Applications.

Dans certains cas particuliers, les évaluations précédentes conduisent au calcul complet de $d(\mathfrak{G}_S)$ et $r(\mathfrak{G}_S)$. Bornons-nous à un exemple (il y en a d'autres dans le texte) :

Supposons que $(S, l) = 1$ (i.e. aucune place $v \in S$ ne divise l), et excluons le cas exceptionnel $S = \emptyset, \delta = 1$. On trouve alors :

Théorème 6. — $r(\mathfrak{G}_S) \leq d(\mathfrak{G}_S) + r$.

En particulier, la différence $r(\mathfrak{G}_S) - d(\mathfrak{G}_S)$ est bornée par le degré du corps k . Plus particulièrement encore, prenons k égal à \mathbf{Q} ou à un corps quadratique imaginaire, et $l \neq 2$. Alors $r = 0$, et l'on trouve $r(\mathfrak{G}_S) \leq d(\mathfrak{G}_S)$. D'autre part, la théorie du corps de classes montre que $\mathfrak{G}_S / (\mathfrak{G}_S, \mathfrak{G}_S)$ est fini. On a donc nécessairement $d(\mathfrak{G}_S) \leq r(\mathfrak{G}_S)$, d'où $d(\mathfrak{G}_S) = r(\mathfrak{G}_S)$.

Problème. — Le groupe \mathfrak{G}_S est-il fini ? (Pour $S = \emptyset$, c'est essentiellement le problème classique de la « tour des corps de classes ».) Vu les résultats précédents, on est tenté de penser que la réponse est négative en général ; on connaît en effet très peu de l -groupes finis ayant autant de générateurs que de relations (en fait, dans les seuls exemples connus, ce nombre est ≤ 3). De façon plus précise, on peut poser la question suivante :

Question. — Pour tout entier $d \geq 0$, soit $r(d)$ le minimum de relations définissant un l -groupe fini à d générateurs. Est-il vrai que $r(d) - d$ tende vers $+\infty$ avec d ?

Si oui, on peut construire des corps de nombres k tels que \mathfrak{G}_S soit infini (avec $S = \emptyset$ si l'on veut).

L'auteur obtient le résultat plus faible suivant : disons qu'un groupe est de hauteur $\leq h$ s'il est extension h -uple de groupes abéliens (i.e. si la suite des commutateurs successifs $G_0 = G, G_{n+1} = (G_n, G_n)$ est telle que $G_h = \{1\}$). Si l'on se borne aux l -groupes finis G de hauteur $\leq h$, on définit comme ci-dessus une fonction $r_h(d)$. Il existe alors une constante $\alpha > 0$ telle que $r_h(d) \leq \alpha d^2$. La démonstration (donnée au § 5) utilise la technique des algèbres de Lie associées aux groupes nilpotents. De là, et du théorème 6, résulte l'existence d'une suite de corps k_i de degrés bornés tels que le « nombre d'étages » de la tour de corps de classes de k_i tende vers l'infini avec i .