Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Thong Nguyen-Quang-Do

Sur le multiplicateur de Schur d'un p-groupe

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 2 (1977-1978), exp. n° 34, p. 1-7

<http://www.numdam.org/item?id=SDPP_1977-1978__19_2_A8_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des Nombres)
19e année, 1977/78, n° 34, 7 p.

20 mars 1978

SUR LE MULTIPLICATEUR DE SCHUR D'UN p-GROUPE

par NGUYEN-QUANG-DO Thong

1. Introduction.

Soit G un groupe fini. Dans l'étude des représentations projectives complexes de G, SCHUR [10] a introduit le multiplicateur $M(G)$, qu'on pourrait définir de façon cohomologique par

$$M(G) = H^2(G, \mathbb{Q}/\mathbb{Z}) \simeq H^3(G, \mathbb{Z}) \quad (G \text{ opérant trivialement}).$$

Citons deux applications arithmétiques du multiplicateur de Schur.

1.1. Le principe des normes de Hasse.

Soit K/k une extension galoisienne de corps de nombres, de groupe de Galois G. Pour toute place v, soit G_v le groupe de Galois de l'extension locale K_v/k_v. Soit $f : M(G) \longrightarrow \prod_v M(G_v)$ le produit des restrictions. Alors

$$\ker f = \frac{\{a \; ; \; a \in K^* , \; a \text{ est une norme locale en toute place } v\}}{\{a \; ; \; a \in K^* , \; a \text{ est une norme globale}\}}$$

(voir, par exemple [2], chap. 7, p. 198).

Pour des exemples de calculs de $\ker f$, voir [1] et [3].

1.2. Le problème de la tour des classes (voir, par exemple [2], chap. 9).

ŠAFAREVIČ a montré que, pour démontrer qu'il existe des corps de nombres dont la tour des classes est infinie, il suffit de prouver la propriété purement algébrique suivante : Pour tout p-groupe G, $\lim_{d(G)\to\infty} d(M(G)) = +\infty$, où $d(.)$ désigne le rang (= nombre minimal de générateurs) d'un groupe.

Or il est facile de voir que, pour tout p-groupe G, $d(M(G)) = r(G) - d(G)$, avec $r(G) = \dim H^2(G, \mathbb{F}_p)$ et $d(G) = \dim H^1(G, \mathbb{F}_p)$. GOLOD et ŠAFAREVIČ ont montré que $r(G) > (d(G)/2)^2$.

En sens inverse, on a l'inégalité de Green [4] :

$$\text{Pour tout groupe } G \text{ d'ordre } p^n , \quad |M(G)| \leq p^{(n(n-1))/2} .$$

En relation avec toutes ces questions, on peut se proposer de chercher à déterminer $M(G)$ en fonction de $M(H)$ et $M(G/H)$, pour tout sous-groupe normal H de G. C'est ce que nous faisons ici, en étendant la suite exacte à cinq termes de Hochschild-Serre en une suite exacte infinie faisant intervenir le "module des relations" de G. La méthode utilisée est d'origine arithmétique. Son principal avantage est de nous dispenser de tout calcul de cocycles et de tout recours aux suites spectrales.

2. Module des relations.

2.1. Définitions. - Soient p un nombre premier, et G un p-groupe. Une présentation (resp. une pro-présentation) de G est une suite exacte

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1 ,$$

où F est un groupe libre (resp. un pro-p-groupe libre) de rang fini. Le rang de F est alors supérieur ou égal à celui de G. S'il est égal, on dit que la présentation est minimale. Le $(\mathbb{Z}G)$-module (resp. $(\mathbb{Z}_p\, G)$-module) $\bar{R} = R/(R , R)$ est appelé module des relations (resp. des pro-relations) de G.

Les modules de relations ont été étudiés par de nombreux auteurs (voir, par exemple [6]). La structure des modules de pro-relations est beaucoup plus simple. Plus précisément, en utilisant :

le théorème de Krull-Schmidt pour les $(\mathbb{Z}_p\, G)$-modules [8],
les théorèmes de Nakayama et D. S. Rim (voir, par exemple [12], chap. 9),
le lemme de Schanuel.

Nous pouvons démontrer alors le résultat suivant.

2.2. THÉORÈME. - *Soit G un p-groupe. Soit I l'idéal d'augmentation de l'algèbre $\mathbb{Z}_p\, G$. Alors :*

(i) *Tout module de pro-relations $\bar{R}$ est semblable au module I^2, i. e. il existe deux $(\mathbb{Z}_p\, G)$-modules libres P_1 et P_2 tels que $\bar{R} \oplus P_1 \simeq I^2 \oplus P_2$.*

(ii) *Soit $\bar{R}_0$ le module des pro-relations d'une pro-présentation minimale de G. Alors le $(\mathbb{Z}_p\, G)$-module $\bar{R}_0$ est indécomposable.*

(iii) *Pour tout module de pro-relations $\bar{R}$, on a*

$$\bar{R} \simeq \bar{R}_0 \oplus (\mathbb{Z}_p\, G)^r , \text{ avec } r = d(F) - d(G) .$$

En vertu de ce théorème, on peut parler du module des pro-relations de G, à équivalence projective près.

3. Un module cohomologiquement trivial.

Soit p un nombre premier, qu'on supposera impair dans tout ce paragraphe. On peut fabriquer arithmétiquement le module des pro-relations d'un p-groupe G grâce à un résultat de Šafarevič.

3.1. THÉORÈME (ŠAFAREVIČ [9]). - *Soit k un corps local p-adique régulier, i. e. une extension finie de $\mathbb{Q}_p$ ne contenant pas les racines p-ièmes de l'unité. Soit F_k le groupe de Galois de la p-extension maximale de k. Alors F_k est un pro-p-groupe libre, tel que*

$$d(F_k) = [k : \mathbb{Q}_0] + 1 .$$

Il résulte en particulier de ce théorème que, si $d(G) \leq d(F_k)$, il existe une

extension galoisienne K/k telle que

$$G \simeq \mathrm{Gal}(K/k) \simeq F_k/R ,$$

où R est le sous-groupe (fermé) de F_k laissant fixe K. La théorie du corps de classes nous donne, en outre, le théorème suivant.

3.2. THÉORÈME. - *Avec les hypothèses et notations précédentes, $\bar{R}/\bar{R}^q$ est isomorphe à $K^\times/K^{\times q}$, pour tout $q = p^n$.*

A partir de cette construction arithmétique, montrons le théorème suivant.

3.3. THÉORÈME. - *Pour tout $q = p^n$, il existe un module de pro-relations $\bar{R}$ du p-groupe G, et un $(\underset{\sim}{Z}_p\, G)$-module A cohomologiquement trivial tels qu'on ait la suite exacte :*

$$0 \longrightarrow \underset{\sim}{Z}/q \longrightarrow A \xrightarrow{q} A \longrightarrow H^1(\bar{R} , \underset{\sim}{Z}/q) \longrightarrow 0 .$$

Preuve. - Réalisons G comme groupe de Galois d'une extension galoisienne K/k comme dans le théorème 3.1. Comme F_k est libre, on peut en plus s'arranger pour que K et $k(\mu_q)$ soient linéairement disjoints (μ_q = groupe des racines q-ièmes de l'unité). Soit σ l'élément d'ordre 2 du groupe $\mathrm{Gal}(k(\mu_q)/k)$, et soit k_1 le corps fixe de σ. Soit K_1 le translaté de K par k_1. L'extension K_1/k_1 est encore une extension galoisienne de corps réguliers, de groupe de Galois isomorphe à G. Soit F le groupe de p-extension maximale de k_1, et soit R le sous-groupe de F laissant fixe K_1.

La démonstration va se faire en plusieurs étapes.

(i) L'opérateur ω (cf. [7], théorèmes). - Dans l'algèbre $\underset{\sim}{Z}_p\langle\sigma\rangle$, considérons l'idempotent $\omega = (1/2)(1 - \sigma)$, et faisons-le opérer sur le groupe $E = 1 + \mathfrak{P}_K$ des unités principales de K. Le résultat suivant est clair.

LEMME 1.

$$E_K = E_{K_1} \times \omega(E_K) \quad (\text{produit direct})$$

(ii) Posons $A = A_K = \omega(E_K)$. Comme ω commute avec G, A_K est un $(\underset{\sim}{Z}_p\, G)$-module.

LEMME 2. - *Le $(\underset{\sim}{Z}_p\, G)$-module A_K est cohomologiquement trivial.*

Pour cela, il suffit de montrer que $H^1(G , A_K) = H^2(G , A_K) = 0$, et l'on voit par récurrence, qu'il suffit de le faire dans le cas où G est cyclique d'ordre p. Supposons donc G cyclique d'ordre p engendré par τ :

(a) Soit $z \in A$ tel que $N_{K/k}(z) = 1$. D'après le théorème 90 de Hilbert, $z = y^{\tau-1}$, $y \in K^\times$. Comme $z \in E_K$, il résulte des propriétés élémentaires de ramification ([12], chap. 4) qu'on peut choisir $y \in E_K$. Alors

$$\omega(z) = z = \omega(y^{\tau-1}) = (\omega(y))^{\tau-1} ,$$

d'où $H^1(G , A_K) = 0$.

(b) Soit $z \in (A_K)^G = A_k$. D'après une propriété connue du corps de classes local ([12], p. 206) pour que z soit une norme de K/k , il faut et il suffit que $N_{k/k_1}(z)$ soit une norme de K_1/k_1 . Mais

$$N_{k/k_1}(z) = N_{k/k_1}(\omega(z)) = \omega N_{k/k_1}(z) = 1 ,$$

donc la propriété est vraie. Donc $z = N_{K/k}(y)$, $y \in K^*$, d'où

$$z = \omega(z) = \omega(N_{K/k}(y)) = N_{K/k}(\omega(y)) \quad \text{et} \quad H^2(G , A_K) = 0 .$$

(iii) Soit ξ une racine primitive q-ième de 1 . Comme $\sigma(\xi) = \xi^{-1}$, $\omega(\xi) = \xi$, donc $\xi \in A$, et l'on a la suite exacte

$$1 \longrightarrow \mu_q \longrightarrow A \longrightarrow A^q \longrightarrow 1 .$$

(iv) Il reste à montrer que $A/A^q \simeq H^1(\bar{R} , \underline{Z}/q)$. Par application de l'opérateur ω , il est immédiat que $A^q = A \cap K^{\times q}$, donc $A/A^q \simeq AK^{\times q}/K^{\times q}$. Soit $\bar{A}$ ce dernier groupe. Par ailleurs, $H^1(\bar{R} , \underline{Z}/q)$ est isomorphe (pour le symbole de Hilbert d'ordre q) à un sous-groupe $\bar{B} = B.K^{\times q}/K^{\times q}$ de $K^\times/K^{\times q}$, et au point de vue galoisien, $\bar{B}$ peut être caractérisé comme suit : Pour tout $b \in K^\times$, $\bar{b} \in \bar{B}$ si, et seulement si, l'extension $K(\sqrt[q]{b})$ est scindée, i. e. provient par translation d'une extension galoisienne de K_1 . Il est bien clair que $\bar{A}$ est un sous-groupe de $\bar{B}$ et que

$$E_K/E_K^q \simeq \bar{A} \times (E_{K_1}/E_{K_1}^q)$$

(en tenant compte du lemme 1).

Mais $|E_{K_1}/E_{K_1}^q| = q^n$, avec $n = [K_1 : \underline{Q}_p]$ et $|E_K/E_K^q| = q^{2n+1}$ (voir, par exemple [12], p. 220), d'où $|\bar{A}| = q^{n+1}$. Comme $\bar{B}$ est dual de $K_1^\times/K_1^{\times q}$ (d'après le théorème 3.2), $|\bar{B}| = |K_1^\times/K_1^{\times q}| = q^{n+1}$, d'où finalement $\bar{A} = \bar{B}$

C. Q. F. D.

3.4. COROLLAIRE. - Pour tout module de pro-relations $\bar{R}$ de G , et, pour tout $n \in \underline{Z}$, on a

$$\hat{H}^n(G , \underline{Z}/q) \simeq \hat{H}^{n-2}(G , H^1(\bar{R} , \underline{Z}/q))$$

(où $\hat{H}$ désigne les groupes de cohomologie modifiés).

Preuve. - C'est immédiat, à partir de 3.3 et 2.2

4. Sur l'inflation-restriction.

Nous allons construire deux suites infinies "dévissant" l'inflation et la restriction.

4.1. THÉORÈME. - Soient G un p-groupe ($p \neq 2$) et H un sous-groupe normal de G . Soit T un module de torsion, G-trivial. Pour tout module de pro-relations $\bar{R}$ de G , on a les suites exactes :

$$0 \longrightarrow H^1(G/H\ ,\ T) \xrightarrow{\inf} H^1(G\ ,\ T) \xrightarrow{\text{res}} H^1(H\ ,\ T)^{G/H} \xrightarrow{\text{tr}} H^2(G/H\ ,\ T)$$
$$\xrightarrow{\inf} H^2(G\ ,\ T)_H \longrightarrow H^1(G/H,\ H^1(H,T)) \longrightarrow H^3(G/H,\ T) \longrightarrow H^1(G/H,\ N_H\ H^1(\bar{R}\ ,\ T))$$
$$\longrightarrow H^2(G/H\ ,\ H^1(H\ ,\ T)) \longrightarrow \ldots \longrightarrow H^n(G/H\ ,\ H^1(H\ ,\ T)) \longrightarrow H^{n+2}(G/H\ ,\ T)$$
$$\longrightarrow H^n(G/H\ ,\ N_H\ H^1(\bar{R}\ ,\ T)) \longrightarrow H^{n+1}(G/H\ ,\ H^1(H\ ,\ T)) \longrightarrow \ldots$$

et

$$0 \longrightarrow H^2(G\ ,\ T)_H \longrightarrow H^2(G\ ,\ T) \xrightarrow{\text{res}} H^2(H\ ,\ T)^{G/H} \xrightarrow{\text{tr}} H^1(G/H\ ,\ N_H\ H^1(\bar{R}\ ,\ T))$$
$$\xrightarrow{\inf} H^3(G\ ,\ T)_H \longrightarrow H^1(G/H\ ,\ H^2(H\ ,\ T)) \longrightarrow H^2(G/H\ ,\ N_H\ H^1(\bar{R}\ ,\ T))$$
$$\longrightarrow H^2(G/H\ ,\ H^1(\bar{R}\ ,\ T)^H) \longrightarrow H^2(G/H\ ,\ H^2(H\ ,\ T)) \longrightarrow \ldots \longrightarrow H^n(G/H\ ,\ H^2(H\ ,\ T))$$
$$\longrightarrow H^{n+1}(G/H\ ,\ N_H\ H^1(\bar{R}\ ,\ T)) \longrightarrow H^{n+1}(G/H\ ,\ H^1(\bar{R}\ ,\ T)^H)$$
$$\longrightarrow H^{n+1}(G/H\ ,\ H^2(H\ ,\ T)) \longrightarrow \ldots$$

où inf désigne l'inflation, res la restriction, tr la transgression, $H^n(.\ ,\ .)_H$ le noyau de la restriction en dimension n, et $N_H = \sum_{\sigma \in H} \sigma$.

Preuve. - Pour simplifier, notons $J = G/H$ et $H^n(.) = H^n(.\ ,\ T)$.

Tout module de torsion étant limite inductive de ses sous-modules finis, il suffit de démontrer le théorème pour $T = \mathbb{Z}/q$. Dans l'énoncé du théorème 3.3, posons $A/A^q = B$. De la suite exacte de G-modules

$$0 \longrightarrow A^q \longrightarrow A \longrightarrow B \longrightarrow 0\ ,$$

où A est cohomologiquement trivial, résulte la suite exacte de J-modules

$$(*) \qquad 0 \longrightarrow (A^q)^H \longrightarrow A^H \longrightarrow N_H\ B \longrightarrow 0\ ,$$

où A^H est cohomologiquement trivial. Soit η l'homomorphisme naturel

$$A^H/(A^H)^q \longrightarrow A/A^q$$

induit par l'injection $A^H \longrightarrow A$. On a les suites exactes naturelles de J-modules

$$0 \longrightarrow (A^H)^q \longrightarrow (A^q)^H \longrightarrow \ker \eta \longrightarrow 0 \quad \text{et} \quad 0 \longrightarrow (A^q)^H \longrightarrow A^H \longrightarrow \operatorname{Im} \eta \longrightarrow 0\ ,$$

d'où $\operatorname{Im} \eta \simeq N_H\ H^1(\bar{R})$ (d'après (*)) et $\operatorname{Ker} \eta \simeq H^1(H)$ (par construction de A).

On obtient alors la première suite exacte du théorème, en écrivant la suite exacte de J-modules

$$0 \longrightarrow \operatorname{Ker} \eta \longrightarrow A^H/(A^H)^q \longrightarrow \operatorname{Im} \eta \longrightarrow 0\ ,$$

et la suite de cohomologie qui en résulte, en tenant compte que

$$H^n(J\ ,\ A^H/(A^H)^q) \simeq H^{n+2}(J) \quad \text{d'après 3.4.}$$

La seconde suite exacte du théorème est la suite de cohomologie correspondant à la suite exacte de J-modules

$$0 \longrightarrow \operatorname{Im} \eta \longrightarrow (A/A^q)^H \longrightarrow H^2(H) \longrightarrow 0$$

(d'après 3.4).

C. Q. F. D.

Des suites exactes du théorème 4.1 résultent immédiatement les corollaires suivants.

4.2. COROLLAIRE 1. - Supposons H central, i. e. inclus dans le centre de G. On a une suite exacte :

$$0 \longrightarrow H^1(G/H\ ,\ T) \xrightarrow{\inf} H^1(G\ ,\ T) \xrightarrow{\mathrm{res}} H^1(H\ ,\ T) \xrightarrow{\mathrm{tr}} H^2(G/H\ ,\ T)$$
$$\xrightarrow{\inf} H^2(G\ ,\ T)_H \longrightarrow H^1(G/H \otimes H\ ,\ T) \longrightarrow H^3(G/H\ ,\ T) \longrightarrow \ldots$$

On retrouve ainsi un résultat de IWAHORI-MATSUMOTO [5].

4.3. COROLLAIRE 2. - Supposons $G = J \times H$. On a une suite exacte scindée :

$$0 \longrightarrow H^2(J\ ,\ T) \longrightarrow H^2(G\ ,\ T)_H \longrightarrow H^1(J \otimes H\ ,\ T) \longrightarrow 0\ .$$

On retrouve ainsi un résultat de YAMAZAKI [13].

4.4. COROLLAIRE 3. - Supposons $G = J \times H$. Alors

$$M(G) \simeq M(J) \times M(H) \times (J \otimes H)\ .$$

C'est un vieux résultat de SCHUR [11]. Il en résulte le corollaire suivant.

4.5. COROLLAIRE 4. - Pour tout p-groupe abélien G tel que $d(G) = d$, on a $r(G) = (d(d+1))/2$.

4.6. COROLLAIRE 5. - Supposons G quelconque, et $J = G/H$ cyclique. Alors

$$|M(G)| \leqslant \frac{|M(H)|\,.\,|\bar{G}|}{|N_J(\bar{H})|}\ .$$

En particulier $|M(G)| \leqslant p^{(n(n-1))/2}$, si $|G| = p^n$ (inégalité de Green).

BIBLIOGRAPHIE

[1] ARMAUDON (M.). - Etude des normes dans les extensions galoisiennes de corps de nombres, C. R. Acad. Sc. Paris, t. 283, 1976, Série A, p. 269-272.

[2] CASSELS (J. W. S.) and FRÖHLICH (A.) [editors]. - Algebraic numbers theory. "Proceedings of an instructional conference, [1965, Brighton]. - London, Academic Press, 1967.

[3] GERTH III (F.). - The Hasse norm principle in metacyclic extensions of number fields, J. London math. Soc., Séries 2, t. 16, 1977, p. 203-208.

[4] GREEN (J. A.). - On the number of automorphisms of a finite group, Proc. Royal Soc. London, Series A, t. 237, 1956, p. 574-581.

[5] IWAHORI (N.) and MATSUMOTO (H.). - Several remarks on projective representations of finite groups, J. of Fac. of Sc., Univ. of Tokyo, Section 1, t. 10, 1963/64, p. 129-146.

[6] LYNDON (R. C.). - Dependance and independance in free groups, J. für reine und angew. Math., t. 210, 1962, p. 148-174.

[7] MIKI (H.). - On some Galois cohomology groups of a local field and its application to the maximal p-extension, J. Math. Soc. Japon, t. 28, 1976, p. 114-122.

[8] REINER (L.). - The Krull-Schmidt for integral group representations, Bull. Amer. math. Soc., t. 67, 1961, p. 365-367.

[9] ŠAFAREVIČ (L. R.). - On p-extensions, Amer. Math. Soc., Translations, Series 2, t. 4, 1956, p. 59-72.

[10] SCHUR (I.). - Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. für reine und angew. Math., t. 127, 1904, p. 20-50.

[11] SCHUR (I.). - Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. für reine und angew. Math., t. 132, 1907, p. 85-137.

[12] SERRE (J. P.). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

[13] YAMAZAKI (K.). - On projective representations and ring extensions of finite groups, J. of Fac. of Sc. Univ. of Tokyo, Section 1, t. 10, 1963/64, p. 147-195.

(Texte reçu le 16 mai 1978)

NGUYEN QUANG DO Thong
49 rue Pierre Valette
92240 MALAKOFF