SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Structure de certains pro-p-groupes

Séminaire N. Bourbaki, 1964, exp. n° 252, p. 145-155

<http://www.numdam.org/item?id=SB_1962-1964__8__145_0>

Séminaire BOURBAKI
15e année, 1962/63, n° 252

Février 1963

STRUCTURE DE CERTAINS PRO-p-GROUPES

par Jean-Pierre SERRE

(d'après DEMUŠKIN [1])

I. Résultats.

1. Pro-p-groupes.

Soit p un nombre premier. Un pro-p-groupe est un groupe topologique qui est limite projective de p-groupes finis ; c'est un groupe compact totalement discontinu.

Exemple. - Soit n un entier, soit $L(n)$ le groupe libre engendré par n éléments, et soit $F(n)$ la limite projective des quotients finis de $L(n)$ qui sont des p-groupes. Le groupe $F(n)$ s'appelle le pro-p-groupe libre de rang n. On a $F(0) = 1$, $F(1) = \underset{\sim}{Z}_p$ (groupe additif des entiers p-adiques).

2. Cohomologie des pro-p-groupes.

Soit G un pro-p-groupe. La cohomologie de G se définit comme dans [2]. Nous aurons surtout à considérer le cas où le groupe des coefficients est $\underset{\sim}{Z}/p\underset{\sim}{Z}$, G opérant trivialement ; les groupes de cohomologie correspondants seront notés $H^q(G)$. On a :

$$H^q(G) = \varinjlim H^q(G/U) \quad ,$$

lorsque U parcourt l'ensemble des sous-groupes ouverts distingués de G .

Les groupes $H^1(G)$ et $H^2(G)$ ont une interprétation simple :

On a $H^1(G) = \mathrm{Hom}(G , \underset{\sim}{Z}/p\underset{\sim}{Z})$. De là, et des propriétés élémentaires des p-groupes finis, on tire :

2.1. - Soient $x_1 , \ldots , x_n \in G$. Pour que les x_i engendrent (topologiquement) le groupe G , il faut et il suffit que tout $f \in \mathrm{Hom}(G , \underset{\sim}{Z}/p\underset{\sim}{Z})$ tel que $f(x_1) = \ldots = f(x_n) = 0$ soit nul.

En particulier, G est isomorphe à un quotient de $F(n)$ si et seulement si $\dim H^1(G) \leq n$.

2.2 (cf. [2], proposition 3.3). - Pour que G soit isomorphe à $F(n)$, il faut et il suffit que $H^2(G) = 0$ et $\dim H^1(G) = n$.

2.3. - Soit $G = F(n)/R$. Supposons que $\dim H^1(G) = n$, et soit $h = \dim H^2(G)$. L'entier h est égal au "nombre de relations" définissant R (nombre minimum d'éléments de R dont les conjugués engendrent un sous-groupe dense dans R).

La démonstration se fait en construisant un isomorphisme $H^1(R)^G \to H^2(G)$, et en montrant (comme pour 2.1) que la dimension de $H^1(R)^G$ est égale au "nombre de relations" engendrant R.

On voit en même temps que tout élément $r \in R$ définit un homomorphisme $\overline{r} : H^2(G) \to \underset{\sim}{Z}/p\underset{\sim}{Z}$, et que des éléments $r_1, \dots, r_k$ ont des conjugués qui engendrent topologiquement R si et seulement si l'intersection des noyaux des $\overline{r}_i$ est réduite à zéro.

3. Les groupes de Demuškin.

Nous dirons qu'un pro-p-groupe G est un groupe de Demuškin s'il vérifie les deux propriétés suivantes :

(i) $H^2(G)$ est de dimension 1 sur le corps $\underset{\sim}{Z}/p\underset{\sim}{Z}$.

(ii) $H^1(G)$ est de dimension finie, et le cup-produit :

$$H^1(G) \times H^1(G) \to H^2(G) = \underset{\sim}{Z}/p\underset{\sim}{Z}$$

est une forme bilinéaire non dégénérée.

On se propose de classer ces groupes. Avant de le faire, il faut en définir deux invariants :

a. L'invariant le plus évident est le rang $n = \dim H^1(G)$. Vu 2.3, le groupe G peut s'écrire comme quotient de $F(n)$ par un sous-groupe distingué fermé $R = (r)$ engendré topologiquement par les conjugués d'un élément r (un groupe de Demuškin est défini par une relation). Il faudra donc classer ces relations, et les mettre sous forme aussi canonique que possible.

b. Soit G_a le quotient de G par l'adhérence (G, G) du groupe des commutateurs. C'est un quotient de $(\underset{\sim}{Z}_p)^n$ par un sous-groupe isomorphe à $\underset{\sim}{Z}_p$, ou réduit à 0. Comme en outre $H^1(G_a) = H^1(G)$ est de dimension n, on en conclut que G_a est isomorphe à $(\underset{\sim}{Z}_p)^n$ ou à $\underset{\sim}{Z}/q\underset{\sim}{Z} \times (\underset{\sim}{Z}_p)^{n-1}$, avec $q = p^f$ $(f \geq 1)$. L'entier q est un invariant de G (on convient que $G_a = (\underset{\sim}{Z}_p)^n$ correspond à $q = 0$).

3.1. THÉORÈME (DEMUŠKIN). - *Supposons que l'invariant* q *de* G *soit* $\neq 2$. *Le groupe* G *est alors déterminé par ses invariants* n *et* q ; *il est isomorphe au groupe défini par* n *générateurs* $x_1, \dots, x_n$ *liés par la relation*

$$x_1^q(x_1, x_2)(x_3, x_4)\dots(x_{n-1}, x_n) = 1 \quad .$$

Remarques :

a. On note (x, y) le commutateur $xyx^{-1}y^{-1}$.

b. L'entier n est nécessairement pair (toujours sous l'hypothèse $q \neq 2$).

c. Lorsque $q = 0$, la relation (3.1) n'est autre que la relation bien connue donnant le groupe fondamental $\pi_1(S)$ d'une surface orientable compacte S. Il serait d'ailleurs facile de prouver directement que le p-complété de $\pi_1(S)$ est un groupe de Demuškin.

Le cas $q = 2$ (i. e. $p = 2$ et $f = 1$) est exceptionnel : les invariants n et q ne suffisent plus à déterminer G (à part, bien sûr, le cas trivial $n=1$, où $G = \mathbb{Z}/2\mathbb{Z}$). Lorsque n est impair, on peut donner une classification complète :

3.2. THÉORÈME. - *Supposons que* $q = 2$ *et* $n = 2m + 1$, *avec* $n \geqslant 1$. *Le groupe* G *est alors isomorphe au groupe défini par* n *générateurs* $x_1, \dots, x_n$ *liés par une relation de la forme* :

$$x_1^2\, x_2^k(x_2, x_3)\dots(x_{2m}, x_{2m+1}) = 1 \quad ,$$

où k *est égal à* 0 *ou à* 2^s (*avec* $s \geqslant 2$). *De plus, des valeurs distinctes de* k *conduisent à des groupes non isomorphes.*

Pour $n = 2$, on a un résultat analogue : le groupe G peut être défini par deux générateurs x, y liés par une relation de la forme

$$yxy^{-1} = x^{-(1+k)} \quad ,$$

k prenant les mêmes valeurs que ci-dessus ; ici encore deux valeurs distinctes de k conduisent à des groupes non isomorphes. Pour n pair et $\geqslant 4$ je ne connais pas de classification complète.

4. Application aux groupes de Galois des corps locaux.

Soit $\mathbb{Q}_p$ le corps p-adique usuel et soit K une extension de $\mathbb{Q}_p$ de degré fini d. Soit $K(p)$ la plus grande extension galoisienne de K dont le groupe de Galois G soit un pro-p-groupe. On désire déterminer la structure de G.

4.1. THÉORÈME (ŠAFAREVIČ [6]). - Si K ne contient pas les racines p-ièmes de l'unité, G est un pro-p-groupe libre de rang $n = d + 1$.

4.2. THÉORÈME. - Soit q la plus grande puissance de p telle que K contienne les racines q-ièmes de l'unité, et supposons $q \neq 1$. Alors G est un groupe de Demuškin d'invariants $(d + 2, q)$.

(En particulier, G est défini par une relation, comme l'avait déjà remarqué KAWADA [3].)

4.3. COROLLAIRE (DEMUŠKIN [1]). - Si $q \neq 2$, le groupe G peut être défini par $d + 2$ générateurs $x_1 , \dots , x_{d+2}$ liés par la relation

$$x_1^q (x_1 , x_2) \dots (x_{d+1} , x_{d+2}) = 1 \quad .$$

Lorsque $q = 2$, on a :

4.4. COROLLAIRE. - Supposons $q = 2$ et d impair. Alors G peut être défini par $d + 2$ générateurs $x_1 , \dots , x_{d+2}$ liés par la relation :

$$x_1^2 x_2^4 (x_2 , x_3) \dots (x_{d+1} , x_{d+2}) = 1 \quad .$$

En particulier, pour $K = \mathbb{Q}_2$, le groupe G est engendré par trois éléments x , y , z liés par la relation

$$x^2 y^4 (y , z) = 1 \quad .$$

II. Démonstrations.

5. Une précision au théorème 3.1.

Le résultat prouvé par DEMUŠKIN est plus précis que le théorème 3.1 en ce sens qu'il détermine la structure d'une relation donnée.

Il s'énonce ainsi :

5.1. THÉORÈME. - Soit $r \in F(n)$, soit $R = (r)$ le sous-groupe distingué fermé engendré par r , et soit $G_r = F(n)/R$. Supposons que G_r soit un groupe de Demuškin d'invariants (n , q) , avec $q \neq 2$. Il existe alors un système de générateurs $x_1 , \dots , x_n$ de F(n) tel que l'on ait :

$$r = x_1^q (x_1 , x_2) \dots (x_{n-1} , x_n) \quad .$$

Lorsque $q = 2$ et $n = 2m + 1$, on a un résultat analogue, qui précise le théorème 3.2.

6. Démonstration du théorème 5.1.

On va se borner, pour simplifier, au cas où $p \neq 2$ et $q \neq 0$. La démonstration utilise de façon essentielle une certaine filtration (F_i) du pro-p-groupe libre $F = F(n)$. Elle est définie ainsi :

$$F_1 = F , \qquad F_{i+1} = (F_i)^q (F , F_i) , \qquad i \geqslant 1 .$$

En fait, la définition suivante (cf. LAZARD [4]) est plus commode : soit A l'algèbre des séries formelles associatives (mais non commutatives) en n lettres $t_1 , \dots , t_n$, et à coefficients dans $\underset{\sim}{Z}_p$; muni de la topologie de la convergence simple des coefficients, A est une $\underset{\sim}{Z}_p$-algèbre compacte. Le groupe multiplicatif U_A^1 des éléments de A de terme constant égal à 1 est un pro-p-groupe, contenant les éléments $1 + t_i$. Si l'on associe aux générateurs x_i de F les $1 + t_i$, on définit un homomorphisme $\varepsilon : F \to U_A^1$; cet homomorphisme est injectif. De plus, si m est l'idéal de A engendré par q et les t_i, on a

$$F_i = \varepsilon^{-1}(1 + m^i) \qquad :$$

la filtration (F_i) est induite par la filtration m-adique de A. Ceci permet de déterminer le gradué associé $gr(F)$ de F : c'est une certaine sous-algèbre de Lie de $gr(A)$. De façon plus précise, pour $p \neq 2$, c'est l'algèbre de Lie libre en n lettres $y_1 , \dots , y_n$, à coefficients dans l'anneau de polynômes $\underset{\sim}{Z}/q\underset{\sim}{Z}[\pi]$, π étant une indéterminée (l'image de q dans $gr_1(A)$) ; la graduation est définie par le fait que π et les y_i sont de degré 1 ; la multiplication par π dans $gr(F)$ est induite par l'élévation à la puissance q-ième dans F.

Soit maintenant r un élément de F tel que le groupe G_r correspondant soit un groupe de Demuškin d'invariants (n , q). On voit tout de suite que r appartient au second terme F_2 de la filtration (F_i). Soit $\overline{r}$ l'image de r dans $gr_2(F) = F_2/F_3$. Vu la structure de $gr(F)$, $gr_2(F)$ a une base (sur $\underset{\sim}{Z}/q\underset{\sim}{Z}$) formée des πy_i et des $[y_k , y_\ell]$ $(k < \ell)$, images respectivement des x_i^q et des (x_k , x_ℓ). Tout $r \in F_2$ a donc une classe $\overline{r} \in F_2/F_3$ qui s'écrit :

$$\overline{r} = \sum a_i \pi y_i + \sum b_{k\ell}[y_k , y_\ell] , \qquad a_i , b_{k\ell} \in \underset{\sim}{Z}/q\underset{\sim}{Z} ,$$

ce qui équivaut à :

$$r \equiv \prod x_i^{qa_i} \prod (x_k , x_\ell)^{b_{k\ell}} \mod F_3 .$$

6.1. LEMME. - Soit $r \in F_2$. Pour que le groupe $G_r = F/(r)$ soit un groupe de Demuškin d'invariants (n , q), il faut et il suffit que :

(i) Les a_i soient premiers entre eux mod q ,

(ii) La matrice alternée b définie par les $(b_{k\ell})$ soit inversible mod q .

On obtient (i) en écrivant que le groupe G_r, rendu abélien, a un groupe de torsion d'ordre exactement q . Pour (ii), on montre que la réduction mod p de la matrice b donne le cup-produit sur $H^1(G)$.

De ce lemme résulte aussitôt (en faisant un changement linéaire sur les y_i):

6.2. LEMME. - Si r vérifie les conditions de 5.1, il existe un système $x_1 , \dots , x_n$ de générateurs de F tel que l'on ait :

$$r \equiv x_1^q (x_1 , x_2) \dots (x_{n-1} , x_n) \mod F_3 \quad .$$

On va maintenant procéder par approximations successives. Notons $r_o(x)$ l'élément $x_1^q (x_1 , x_2) \dots (x_{n-1} , x_n)$, et supposons trouvés des générateurs $x_1, \dots, x_n$ tels que

$$r \equiv r_o(x) \mod F_h , \quad h \geqslant 3 \quad .$$

On va voir que l'on peut modifier les x_i de telle sorte que cette relation soit vraie mod F_{h+1} . De façon plus précise, soit $c = (c_1 , \dots , c_n)$ un système d'éléments de F_{h-1} , et posons $x_i = x_i' c_i$; les x_i' sont encore des générateurs de F . Ecrivons $r_o(x)$ sous la forme $r_o(x') d(c)$, avec $d(c) \in F$. On voit tout de suite que le terme correctif $d(c)$ appartient à F_h , et que son image $\overline{d}(c)$ dans $gr_h(F)$ ne dépend que des images $(\overline{c}_1 , \dots , \overline{c}_n)$ des c_i dans $gr_{h-1}(F)$. On a ainsi défini une application

$$\overline{d} : (gr_{h-1}(F))^n \to gr_h(F) \quad ,$$

application qui est d'ailleurs un homomorphisme.

6.3. LEMME. - L'application $\overline{d} : (gr_{h-1}(F))^n \to gr_h(F)$ est surjective pour $h \geqslant 2$.

On identifie $gr(F)$ à l'algèbre de Lie libre sur $\mathbb{Z}/q\mathbb{Z}[\pi]$, et l'on calcule $\overline{d}$. On trouve :

$$\overline{d}(\overline{c}_1 , \dots , \overline{c}_n) = \pi . \overline{c}_1 + [\overline{c}_1 , y_2] + [y_1 , \overline{c}_2] + \dots + [y_{n-1} , \overline{c}_n] \quad .$$

C'est suffisamment explicite pour que la surjectivité de $\overline{d}$ se voie sans trop de mal ...

Le lemme 6.3 permet de passer de h à h + 1 : Si l'on a $r = r_o(x) . u$, avec

$u \in F_h$, on choisit c de telle sorte que $d(c) \equiv u^{-1} \mod F_{h+1}$, et en passant aux x_i' , on a $r \equiv r_o(x') \mod F_{h+1}$. On itère cette construction, et on passe à la limite (c'est possible puisque les corrections successives c tendent vers 1). On obtient alors $r = r_o(x)$, ce qui achève de démontrer le théorème 5.1.

Remarques.

a. Lorsque $q = 0$, on filtre F au moyen de la suite centrale descendante. Le gradué associé est l'algèbre de Lie libre à coefficients dans $\underset{\sim}{Z}_p$; la démonstration ci-dessus se simplifie un peu (du fait que les puissances q-ièmes et l'élément π ont disparu).

b. Lorsque $q = 2^f$, avec $f \geqslant 2$, le groupe $gr(F)$ n'est plus tout à fait une algèbre de Lie libre ; toutefois, on peut montrer que le lemme 6.3 reste vrai, et c'est l'essentiel.

7. Démonstration du théorème 3.2.

Il s'agit du cas exceptionnel $q = p = 2$. On se bornera à de brèves indications.

La filtration (F_i) de F est la même que ci-dessus :

$$F_1 = F \ , \quad F_{i+1} = (F_i)^2 \ (F \ , \ F_i) \qquad ,$$

et la méthode de Lazard s'applique encore. Il s'ensuit que $gr(F)$ se plonge comme sous-algèbre de Lie dans $gr(A)$. Mais ici l'application $x \to x^2$ ne correspond plus, par passage à $gr(A)$, à la multiplication par π ; il en résulte que $gr(F)$ n'est plus une algèbre sur $\underset{\sim}{Z}/2\underset{\sim}{Z}[\pi]$. Cela n'empêche pas de déterminer explicitement $gr(F)$.

En particulier, si $r \in F_2$ définit un groupe de Demuškin, un argument analogue à celui du lemme 6.1 montre qu'il existe des générateurs x_i tels que :

$$(7.1) \qquad r \equiv x_1^2 (x_2 \ , \ x_3) \ldots (x_{n-1} \ , \ x_n) \mod F_3 \qquad (n \text{ impair})$$

ou encore :

$$(7.2) \qquad r \equiv x_1^2 \, x_2^2 \ldots x_n^2 \mod F_3 \qquad (n \text{ quelconque}) \qquad .$$

A partir de là, on procède par approximations successives, comme ci-dessus. On définit $\overline{d}$: $(gr_{h-1}(F))^n \to gr_h(F)$, mais cette application n'est pas surjective. Tout ce que l'on peut affirmer, c'est que (une fois (7.1) vérifié) $gr_h(F)$ est engendré par l'image de $\overline{d}$ et par les classes des éléments $x_2^{2^h}$, ... , $x_n^{2^h}$. On en déduit facilement que l'on peut mettre r sous la forme

$$r = r_0 . x_2^{\mu_2} \cdots x_n^{\mu_n} , \qquad \text{(pour } n \text{ impair)}$$

avec $r_0 = x_1^2(x_2 , x_3)\cdots(x_{n-1} , x_n)$, les μ_i étant des entiers 2-adiques divisibles par 4 .

Cette expression de r peut aussi s'écrire :

$$r = x_1^2 . r' \text{ , avec } r' = (x_2 , x_3)\cdots(x_{n-1} , x_n)\, x_2^{\mu_2} \cdots x_n^{\mu_n} .$$

La relation r' ne contient que les variables $x_2 , \ldots , x_n$, et c'est une relation "de Demuškin" par rapport à ces variables ; de plus, son invariant q est nul ou ≥ 4 . On peut donc lui appliquer le théorème 5.1, et choisir $x_2,\ldots,x_n$ de telle sorte que :

$$r' = x_2^k(x_2 , x_3)\cdots(x_{n-1} , x_n) ,$$

où k est égal à 0 ou à 2^s $(s \geq 2)$. Comme $r = x_1^2 r'$, on a bien mis r sous la forme cherchée, ce qui démontre la première partie du théorème.

Il reste à voir que les groupes G_k correspondant à des valeurs distinctes de k ne sont pas isomorphes. Pour cela, on utilise l'homomorphisme canonique

$$\chi : G_k \to U_2$$

associé au module dualisant du groupe G_k (cf. n° 9). Un calcul sans difficultés montre que l'on a $\chi(x_1) = -1$, $\chi(x_3) = 1 + k$, et que $\chi(x_i) = 1$ pour $i \neq 1 , 3$. L'image de G_k par χ est donc égale au groupe $\{\pm 1\} \times C_k$, où C_k désigne le sous-groupe de U_2 formé des éléments congrus à 1 mod k . Comme ces sous-groupes sont deux à deux distincts, il en résulte bien que les groupes G_k sont deux à deux non isomorphes.

8. Démonstration des résultats du n° 4 (corps locaux).

On laisse de côté le théorème 4.1, qui est bien connu (cf. [3], [6]). Pour prouver 4.2, on utilise la suite exacte

$$0 \to \underset{\sim}{Z}/p\underset{\sim}{Z} \to K(p)^* \to K(p)^* \to 0 .$$

Par passage à la cohomologie, elle fournit la suite exacte :

$$0 \to H^2(G) \to H^2(G , K(p)^*) \xrightarrow{p} H^2(G , K(p)^*) .$$

On a $H^2(G , K(p)^*) = \underset{\sim}{Q}_p/\underset{\sim}{Z}_p$: cela résulte du calcul du groupe de Brauer d'un corps local (voir par exemple [7], chapitre XIII). On a donc $H^2(G) = \underset{\sim}{Z}/p\underset{\sim}{Z}$. D'autre part, on voit facilement que $H^1(G)$ s'identifie au quotient K^*/K^{*p} , le cup-produit correspondant au symbole (a , b) de Hilbert (cf. [7], chapitre XIV). Il est bien connu que ce symbole est non dégénéré, d'où le fait que G est un groupe de Demuškin. De plus, la théorie du corps de classes local montre

que G_a est isomorphe à la p-complétion du groupe K^*, c'est-à-dire au produit de $\underset{\sim}{Z}/q\underset{\sim}{Z}$ par $(\underset{\sim}{Z}_p)^{d+1}$. Les invariants de G sont donc $d+2$ et q, ce qui achève de prouver le théorème 4.2 et le corollaire 4.3.

Pour démontrer 4.4, on remarque d'abord que le module dualisant de G est la composante p-primaire du groupe des racines de l'unité. Lorsque $p = 2$ et que d est impair, on a $q = 2$, et l'homomorphisme canonique $\chi : G \to U_2$ est surjectif. Ceci entraîne $k = 4$ (avec les notations de 3.2), d'où le résultat cherché.

III. Compléments.

9. Autres propriétés des groupes de Demuškin.

Soit G un groupe de Demuškin infini (ce qui écarte le cas trivial $G = \underset{\sim}{Z}/2\underset{\sim}{Z}$, et revient à demander que $n \geqslant 2$). On a alors les propriétés suivantes, qui m'ont été communiquées par TATE :

9.1. G est de dimension cohomologique 2.

[En d'autres termes, on a $H^q(G, A) = 0$ pour $q \geqslant 3$ lorsque A est un G-module de torsion, cf. [2].]

Esquissons la démonstration. Soit C la catégorie des G-modules finis annulés par p. Si $M \in C$, soit $M' = \mathrm{Hom}(M, \underset{\sim}{Z}/p\underset{\sim}{Z})$ le dual de M ; le cup-produit définit un accouplement entre $H^i(G, M)$ et $H^{2-i}(G, M')$, autrement dit un homomorphisme $\alpha_i : H^i(G, M) \to (H^{2-i}(G, M'))'$. Ces homomorphismes sont des isomorphismes pour $M = \underset{\sim}{Z}/p\underset{\sim}{Z}$ et $i = 0, 1, 2$. Par dévissage, on en déduit que, pour tout $M \in C$, α_0 est surjectif, α_1 bijectif et α_2 injectif. D'autre part, du fait que G est infini, on peut montrer que le foncteur $H^0(G,)$ est coeffaçable : pour tout $M \in C$, il existe $M_1 \in C$ et une surjection $M_1 \to M$ tel que l'homomorphisme $H^0(G, M_1) \to H^0(G, M)$ soit nul. Combinant ces résultats, on voit que α_i est un isomorphisme pour tout $M \in C$ et $i = 0, 1, 2$. En particulier le foncteur $H^2(G,)$ est exact à droite sur C ; il en résulte facilement que $H^3(G, M) = 0$ pour tout $M \in C$, d'où 9.1.

9.2. Tout sous-groupe ouvert H de G est un groupe de Demuškin.

On ramène la cohomologie de H à celle de G, grâce à la formation des "modules induits", cf. [2], et on applique le théorème de dualité démontré ci-dessus.

[Si les rangs de G et H sont respectivement n_G et n_H, et si $d = (G:H)$, un calcul de caractéristiques d'Euler-Poincaré montre que $n_H - 2 = d(n_G - 2)$.]

9.3. Il existe un homomorphisme unique $\chi : G \to U_p$ (groupe des unités p-adiques) tel que, si l'on fait opérer G sur $\mathbb{Q}_p/\mathbb{Z}_p$ au moyen de χ, le module I ainsi obtenu ait les propriétés suivantes :

a. $H^2(G , I) = \mathbb{Q}_p/\mathbb{Z}_p$.

b. Si M est un G-module fini p-primaire, et si l'on pose $M' = \mathrm{Hom}(M , I)$, le cup-produit met en dualité les groupes finis $H^i(G , M)$ et $H^{2-i}(G , M')$, pour $i = 0 , 1 , 2$.

Le module I est appelé le module dualisant de G. Son existence et ses propriétés peuvent se démontrer pour tout pro-p-groupe G dont l'algèbre de cohomologie $H^*(G)$ vérifie la dualité de Poincaré pour une certaine dimension ; il n'est pas nécessaire que cette dimension soit égale à 2.

L'homomorphisme χ est un invariant intéressant du groupe G (il rend inutile l'invariant q : en effet, q est la plus grande puissance de p telle que l'image de χ soit formée d'éléments congrus à 1 mod q). On peut caractériser χ par la propriété suivante :

Si l'on fait opérer G sur $\mathbb{Z}/p^n\mathbb{Z}$ au moyen de χ, le G-module I_n ainsi obtenu est tel que l'homomorphisme

$$H^1(G , I_n) \to H^1(G , I_1) = H^1(G)$$

soit surjectif (pour tout $n \geq 1$). C'est cette caractérisation que l'on utilise pour déterminer explicitement χ lorsque la relation r définissant G est connue.

10. Questions.

10.1. Classifier les groupes de Demuškin lorsque n est pair et $p = 2$. Sont-ils encore caractérisés par n et $\mathrm{Im}(\chi)$?

10.2. Soit $r \in F_2$, et soit $G_r = G/(r)$. Peut-on étendre à G_r les résultats démontrés par LYNDON [5] dans le cas discret ? En particulier, si r n'est pas une puissance p-ième, est-il vrai que G est de dimension cohomologique 2 ?

BIBLIOGRAPHIE

[1] DEMUŠKIN (S.). - Le groupe de la p-extension maximale d'un corps local [en russe], Dokl. Akad. Nauk S. S. S. R., t. 128, 1959, p. 657-660.

[2] DOUADY (A.). - Cohomologie des groupes compacts totalement discontinus, Séminaire Bourbaki, t. 12, 1959/60, exposé 189, 12 p.

[3] KAWADA (Y.). - On the structure of the Galois group of some infinite extensions, I., J. Fac. Sc., Univ. Tokyo, t. 7, 1954, p. 1-18.

[4] LAZARD (M.). - Sur les groupes nilpotents et les anneaux de Lie, Ann. scient. Ec. Norm. Sup., t. 71, 1954, p. 101-190.

[5] LYNDON (R.). - Cohomology theory of groups with a single defining relation, Annals of Math., Series 2, t. 52, 1950, p. 650-665.

[6] ŠAFAREVIČ (I.). - Sur les p-extensions [en russe], Math. Sbornik, N. S., t. 20, 1947, p. 351-363 [Amer. Math. Soc. Transl., Series 2, t. 4, p. 59-72].

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