SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Cohomologie et arithmétique

Séminaire N. Bourbaki, 1954, exp. n° 77, p. 263-269

<http://www.numdam.org/item?id=SB_1951-1954__2__263_0>

© Association des collaborateurs de Nicolas Bourbaki, 1954, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) 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/

Séminaire BOURBAKI
(Février 1953)

COHOMOLOGIE ET ARITHMÉTIQUE

par Jean-Pierre SERRE

La cohomologie des groupes joue un rôle de plus en plus grand en théorie du corps de classes, aussi bien pour en exprimer les résultats que pour les démontrer. Les articles de HOCHSCHILD [2] (dans le cas local) et de WEIL [6] (cas global) avaient déjà montré l'utilité des groupes de cohomologie du groupe de Galois d'une extension K/k, les coefficients étant, soit le groupe multiplicatif K^* (dans le cas local), soit le groupe C_K des classes d'idèles de K (dans le cas global). Ces derniers groupes ont été déterminés, pour les dimensions 1 et 2, par HOCHSCHILD-NAKAYAMA [3], et J. TATE [5] a montré récemment que leur détermination complète pouvait s'effectuer à partir de là par voie purement algébrique.

Nous démontrerons le théorème de Tate au paragraphe 2, et dans les paragraphes 3, 4 nous en indiquerons rapidement quelques applications. Pour plus de détails, le lecteur pourra se reporter à [1], I et II.

1. Cohomologie des groupes : rappel.

1.1. Notations.- Dans ce qui suit, G désignera un groupe fini, abélien ou non. Un groupe abélien A sur lequel G opère à gauche sera dit un G-module, et l'on posera :

NA = ensemble des $\sum_{g \in G} g.a$, pour $a \in A$ ($\sum_{g \in G} g.a = N(a)$ est la norme de a).
QA = ensemble des $a \in A$, avec $N(a) = 0$.
DA = sous-groupe engendré par les $a - g.a$, $a \in A$, $g \in G$.
FA = ensemble des $a \in A$, avec $g.a = a$ pour tout $g \in G$.

Lorsque le groupe G devra être précisé, on écrira $N_G A$, ..., au lieu de NA, ... Les NA, QA, DA, FA sont des sous-groupes de A, et l'on a :

$$NA \subset FA \quad , \quad DA \subset QA \quad .$$

1.2.- Un G-module A est dit fin (ou G-fin, si l'on veut spécifier G) s'il existe un sous-groupe B de A tel que A soit somme directe des $g.B$, pour $g \in G$. Si A est G-fin, il est a fortiori U-fin pour tout sous-groupe U de G.

Définition équivalente : A est isomorphe à $Z(G) \otimes B$, où $Z(G)$ désigne l'algèbre du groupe G sur l'anneau Z des entiers.

Lorsque A est fin, on voit tout de suite que $NA = FA$ et $DA = QA$.

1.3.- Soit A un G-module. On définit classiquement les groupes d'homologie et de cohomologie de G à coefficients dans A , notés $H_i(G , A)$ et $H^i(G , A)$. Nous n'en répèterons pas la définition, renvoyant à HOPF, EILENBERG-MACLANE, etc. Pour $i = 0$, nous nous écarterons de la définition habituelle, et nous poserons :

$$\begin{cases} H^0(G , A) = FA/NA & \text{(au lieu de } FA) \\ H_0(G , A) = QA/DA & \text{(au lieu de } A/DA) . \end{cases}$$

1.4.- Suite exacte de cohomologie.- Soit $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ une suite exacte de G-modules. Au moyen de la norme, on définit un homomorphisme canonique de $H_0(G , C)$ dans $H^0(G , A)$, et l'on vérifie directement que la suite :

$$H_0(G , A) \longrightarrow H_0(G , B) \longrightarrow H_0(G , C) \longrightarrow H^0(G , A) \longrightarrow H^0(G , B) \longrightarrow H^0(G , C)$$

est exacte. Ceci conduit, avec TATE, à poser $H_0(G , A) = H^{-1}(G , A)$, et plus généralement, $H_i(G , A) = H^{-i-1}(G , A)$; on obtient donc des groupes de cohomologie de dimension négative, et la suite exacte :

$$\ldots \longrightarrow H^i(G , A) \longrightarrow H^i(G , B) \longrightarrow H^i(G , C) \longrightarrow H^{i+1}(G , A) \longrightarrow \ldots ,$$

est valable pour $-\infty < i < +\infty$.

1.5.- Si A est fin, il est classique que $H^i(G , A) = 0$ pour $-\infty < i < +\infty$.

1.6.- Soit A un G-module arbitraire, et soit $B = Z(G) \otimes A$, où G opère par $g.(z \otimes a) = g.z \otimes a$. Posons $\varphi(g \otimes a) = g.a$; ceci définit un homomorphisme φ de B sur A ; soit C le noyau de φ . Comme B est fin, la suite exacte de cohomologie montre que :

$$H^i(G , C) \approx H^{i-1}(G , A) \quad \text{pour tout } i .$$

1.7.- On peut inversement plonger A dans B en posant :

$$\psi(a) = \sum_{g \in G} g^{-1} \otimes g.a \quad , \text{ pour tout } a \in A .$$

Posons $D = B/A$. On a alors :

$$H^i(G , D) \approx H^{i+1}(G , A) \quad \text{pour tout } i .$$

Les constructions 1.6 et 1.7 sont utilisées pour "décaler" les groupes de cohomologie. On notera qu'elles valent pour tout sous-groupe U de G , puisque B est U-fin.

2. Le théorème de Tate.

Dans tout ce paragraphe, G désigne un groupe fini, A un G-module.

2.1. LEMME.- *Pour tout nombre entier* p , *soit* G_p *un sous-groupe de Sylow de* G , *relatif à* p . *Si* $H^i(G_p , A) = 0$ *pour tout* p , *alors* $H^i(G , A) = 0$.

Par décalage, on peut supposer que $i = 0$, et l'on est ramené à un calcul élémentaire sur les normes.

2.2. LEMME.- *Si, pour un entier* i , *on a* $H^i(U , A) = H^{i+1}(U , A) = 0$ *pour tout sous-groupe* U *de* G , *alors* $H^j(G , A) = 0$ *pour tout* j .

A cause du lemme précédent, on peut supposer G résoluble ; si G est cyclique on sait que $H^j(G , A)$ ne dépend que de la parité de j , donc le lemme est vrai dans ce cas. Nous pouvons donc supposer que G contient un sous-groupe invariant U tel que le lemme soit vrai pour U et pour G/U . En outre, à cause du décalage, il nous suffit de prouver que, lorsque $i = 0$, on a $H^{-1}(G , A) = H^2(G , A) = 0$.

Le groupe G/U opère sur $F_U A$, et on voit facilement que le couple $(G/U , F_U A)$ vérifie les hypothèses 2.2 , donc que $H^j(G/U , F_U A) = 0$ pour tout j ; d'autre part, $H^j(U , A) = 0$ pour tout j . En utilisant les relations qui lient les groupes de cohomologie de G , U et G/U (voir par exemple [4]), on en tire bien que $H^{-1}(G , A) = 0$ et $H^2(G , A) = 0$.

2.3. LEMME.- *Supposons que* $H^{-1}(U , A) = 0$, *et que* $H^0(U , A)$ *soit cyclique de même ordre que* U , *pour tout sous-groupe* U *de* G . *Alors* $H^i(G , A) \approx H^i(G , Z)$ *pour tout* i , Z *désignant le groupe additif des entiers sur lequel* G *opère trivialement.*

Soit $a \in FA$ un élément dont l'image dans $FA/NA = H^0(G , A)$ soit un générateur de ce dernier groupe. On voit facilement que l'image de a dans $H^0(U , A)$ est un élément d'ordre égal à l'ordre de U , donc est un générateur de $H^0(U , A)$. Soit $f : Z \longrightarrow A$ l'application $n \longrightarrow n.a$. Pour tout U , f définit donc un isomorphisme de $H^0(U , Z)$ sur $H^0(U , A)$. Soit A' la somme directe de Z(G) et de A , et plongeons Z dans A' par $n \longrightarrow (n.\varepsilon , f(n))$, où $\varepsilon = \sum_{g \in G} g \in Z(G)$. Soit $C = A'/Z$; on a la suite exacte :

$$H^{-1}(U , A') \longrightarrow H^{-1}(U , C) \longrightarrow H^0(U , Z) \longrightarrow H^0(U , A') \longrightarrow H^0(U , C) \longrightarrow H^1(U , Z).$$

Puisque Z(G) est U-fin, on a $H^i(U , A') \approx H^i(U , A)$ pour tout i , d'où $H^{-1}(U , A') = 0$, et $H^0(U , Z) \approx H^0(U , A')$; comme en outre $H^1(U , Z) = 0$

c'est le groupe des homomorphismes de U dans Z, la suite exacte précédente montre que $H^{-1}(U, C) = H^0(U, C) = 0$, d'où (lemme 2.2) $H^i(G, C) = 0$ pour tout i, d'où par suite exacte :

$$H^i(G, Z) \approx H^i(G, A') \approx H^i(G, A), \qquad \text{C.Q.F.D.}$$

Par décalage de deux unités, on tire de là le théorème de Tate :

2.4. THÉORÈME.- Supposons que $H^1(U, A) = 0$ et que $H^2(U, A)$ soit cyclique de même ordre que U, pour tout sous-groupe U de G. Alors $H^i(G, A) \approx H^{i-2}(G, Z)$ pour tout i.

2.5. COROLLAIRE. - $FA/NA \approx G/G'$ (on note G' le groupe des commutateurs de G).

En effet $FA/NA = H^0(G, A)$, et $G/G' = H_1(G, Z) = H^{-2}(G, Z)$.

2.6. COROLLAIRE. - $H^3(G, A) = 0$.

En effet $H^1(G, Z) = 0$.

2.7. COROLLAIRE. - $H^4(G, A) \approx \hat{G}$ (groupe des caractères de degré 1 de G).

En effet $H^2(G, Z) = \mathrm{Ext}(H_1(G, Z), Z) \approx \hat{G}$.

Signalons que l'isomorphisme du Corollaire 2.5 peut être obtenu ainsi : on prend un cocycle $a(s, t)$ sur G, à valeurs dans A, dont la classe de cohomologie engendre $H^2(G, A)$ et l'on pose $\theta(t) = \sum_{s \in G} a(s, t)$; par passage au quotient, θ définit l'isomorphisme de G/G' sur FA/NA.

3. Cas local.

Soit k un corps local, c'est-à-dire un corps valué localement compact non discret. Si l'on excepte $k = R$ et $k = C$, la valuation de k est non archimédienne, son groupe des ordres est Z, et son corps des restes est fini. Si la caractéristique de k est 0, k est une extension finie d'un corps p-adique Q_p ; si la caractéristique de k est p, k est isomorphe au corps des séries formelles à une variable sur son corps des restes.

Soit K une extension galoisienne finie de k, de groupe de Galois G. Le groupe G opère sur le groupe multiplicatif K^* des éléments non nuls de K, qui est donc un G-module, et l'on peut parler des groupes $H^i(G, K^*)$. D'après un résultat général de théorie de Galois, $H^1(G, K^*) = 0$. Le groupe $H^2(G, K^*)$ est cyclique de même ordre que G : ce fait constitue le résultat principal de la théorie du corps de classes local. On le démontre (Cf. [2], ainsi que SCHILLING,

Valuations) en se ramenant, grâce aux "deux inégalités", au cas où K est non ramifié (on peut éviter la seconde inégalité en utilisant le résultat suivant, dû à S. LANG : l'extension maximale non ramifiée de k est quasi-algébriquement close). En outre, $H^2(G , K^*)$ a un générateur canonique, qui correspond à la substitution $x \longrightarrow x^q$, où q est le nombre d'éléments du corps des restes de k .

Le couple (G , K^*) vérifie donc les hypothèses du théorème 2.4 ; en particulier, on a $G/G' \approx FK^*/NK^* = k^*/NK^*$. On sait que ce résultat, combiné avec les théorèmes d'existence, conduit à la détermination du groupe de Galois de l'extension abélienne maximale de k : c'est le complété de k^* pour une certaine topologie.

Le groupe $H^2(G , K^*)$ a une interprétation simple dans la théorie des algèbres : c'ost le groupe des classes d'algèbres simples, de centre k , décomposées par K . En faisant croître K , on obtient donc la détermination du groupe de Brauer $\mathcal{G}_k$ de k : $\mathcal{G}_k \approx \mathbb{Q}/\mathbb{Z}$, groupe des rationnels mod 1 (sauf, bien entendu, si $k = R$ ou C !) .

4. Cas global.

Soit k un corps de nombres algébriques ; pour toute valuation v de k (archimédienne ou non) soit k_v le complété de k pour v ; k_v est un corps local. Soit J_k le sous groupe de $\prod_v k_v^*$ formé des (x_v) tels que x_v soit une unité de k_v pour tout v , sauf un nombre fini (v parcourant l'ensemble de toutes les valuations essentiellement distinctes de k). J_k est le groupe des idèles de k ; si $x \in k^*$, et si l'on pose $x_v = x$ pour tout v , on obtient un idèle principal de J_k ; on peut identifier k^* au sous-groupe des idèles principaux ; le groupe quotient $C_k = J_k/k^*$ est appelé groupe des classes d'idèles.

Si K est une extension galoisienne finie de k , de groupe de Galois G , on peut identifier J_k au sous-groupe des éléments de J_K laissés fixes par G , et de même pour C_k (pour J_k , c'est évident ; pour C_k , cela résulte de la nullité de $H^1(G , K^*)$).

Le résultat principal de la théorie du corps de classes global est alors le suivant :

4.1.- Le couple (G , C_K) vérifie les hypothèses du théorème 2.4. - Autrement dit, on a $H^1(G , C_K) = 0$, et $H^2(G , C_K)$ est cyclique de même ordre que G .

Pour la démonstration, voir [1] , II, ainsi que [3] . Indiquons simplement que

la suite exacte suivante y joue un rôle essentiel :

$$\ldots \longrightarrow H^1(G\ ,\ J_K) \longrightarrow H^1(G\ ,\ C_K) \longrightarrow H^2(G\ ,\ K^*) \longrightarrow H^2(G\ ,\ J_K) \longrightarrow H^2(G\ ,\ C_K) \longrightarrow H^3(G, K^*)$$

Les groupes $H^i(G\ ,\ J_K)$ peuvent facilement être déterminés : pour toute valuation v sur k , choisissons une valuation v^* de K prolongeant v ; et soit G_{v^*} le sous-groupe de G formé des automorphismes qui conservent v^* ("groupe de décomposition" de v^*) ; G_{v^*} est le groupe de Galois de l'extension locale K_{v^*}/k_v , et l'on a :

4.2. - $H^i(G\ ,\ J_K) = \prod{}' H^i(G_{v^*}\ ,\ K^*_{v^*})$, le signe $\prod'$ indiquant que l'on se borne aux éléments qui n'ont qu'un nombre fini de composantes non nulles.

En particulier, $H^1(G\ ,\ J_K) = 0$, donc le fait que $H^1(G\ ,\ C_K) = 0$ équivaut au théorème de Hasse : toute classe d'algèbres simples décomposée localement est décomposée globalement.

On voit de même que le groupe $H^2(G\ ,\ J_K)$ est isomorphe au groupe des fonctions $f(v)$, à valeurs dans $\mathbb{Q}/\mathbb{Z}$, nulles pour tout v sauf un nombre fini, et telles que $n_v.f(v) = 0$, $n_v = [K_{v^*} : k_v]$ = ordre de G_{v^*} ; $H^2(G\ ,\ K^*)$ est isomorphe au sous-groupe du groupe précédent formé des fonctions $f(v)$ telles que $\sum_v f(v) = 0$, et il en résulte que l'image de $H^2(G\ ,\ J_K)$ dans $H^2(G\ ,\ C_K)$ est cyclique d'ordre le ppcm des n_v ; compte tenu de 4.1 , $H^3(G\ ,\ K^*)$ est donc cyclique d'ordre $n/\mathrm{ppcm}(n_v) = \mathrm{pgcd}(n/n_v)$.

CONSÉQUENCE DE 4.1 :

4.3. - D'après 2.5 , $G/G' \approx C_k/NC_K \approx J_k/k^*\ .\ NJ_K$. C'est ce résultat qui permet de montrer que le groupe de Galois de l'extension abélienne maximale de k est isomorphe au quotient de C_k par sa composante connexe de l'unité.

4.4. - Cherchons à quelle condition un élément de k^* , qui est une norme dans tous les k_v^* , est une norme globale (généralisation du théorème de Hasse). Cela revient à voir si $H^0(G\ ,\ K^*) \longrightarrow H^0(G\ ,\ J_K)$ est biunivoque, ou encore si $H^{-1}(G\ ,\ J_K)$ est appliqué sur $H^{-1}(G\ ,\ C_K)$. Or le premier groupe est isomorphe à $\prod{}' H^{-1}(G_{v^*}\ ,\ K^*_{v^*}) = \prod{}' H^{-3}(G_{v^*}\ ,\ Z)$, d'après la théorie locale ; le second est isomorphe à $H^{-3}(G\ ,\ Z)$. Les groupes de caractères de ces deux groupes sont donc respectivement $\prod H^3(G_{v^*}\ ,\ Z)$ et $H^3(G\ ,\ Z)$, et l'on obtient ainsi la condition nécessaire et suffisante suivante (due à Tate) : <u>toute classe de cohomologie entière de degré 3 de G qui induit 0 sur tous les groupes de décomposition doit être nulle</u>. Cette condition est notamment vérifiée si $H^3(G\ ,\ Z) = 0$.

BIBLIOGRAPHIE

[1] ARTIN (E.). - Algebraic numbers and algebraic functions, I. - Princeton University and New York University, 1951 ; II. - à paraître.

[2] HOCHSCHILD (G.). - Local class field theory, Ann. of Math., t. 51, 1950, p. 331-347 (voir aussi l'exposé de Samuel, Séminaire Bourbaki, t. 3, 1950/51).

[3] HOCHSCHILD (G.) and NAKAYAMA (T.). - Cohomology in class field theory, Ann. of Math., t. 55, 1952, p. 348-366.

[4] HOCHSCHILD (G.) and SERRE (J.-P.). - Cohomology of group extensions, Amer. math. Soc., t. 74, 1953, p. 110-134.

[5] TATE (J.). - The higher dimensional cohomology groups of class field theory, Ann. of Math., t. 56, 1952, p. 294-297.

[6] WEIL (André). - Sur la théorie du corps de classes, J. math. Soc. Japan, t. 3, 1951, p. 1-35.

ADDITIF

[7] CHEVALLEY (Claude). - Class field theory. - Nagoya, Nagoya University, 1954. [Cet article contient les démonstrations d'à peu près tous les résultats du présent exposé].

[8] CARTAN (Henri) and EILENBERG (Samuel). - Homological algebra. - Princeton, Princeton University Press, 1956 (Princeton mathematical Series n° 19). [Le chapitre 12 contient une étude de la cohomologie des groupes finis].

Pour d'autres applications du théorème de Tate (et de la notion de "class-formation"), voir :

[9] KAWADA (Y.). - Class formations, I, Duke math. J., t. 22, 1955, p. 165-178 ; II (en collaboration avec I. Satake), J. Fac. Sc. Tokyo, t. 7, 1955, p. 353-389 ; III, J. math. Soc. Japan, t. 7, 1955, p. 453-490.

[10] KAWADA (Y.) and TATE (J.). - On the Galois cohomology of unramified extensions of functions fields in one variable, Amer. J. of Math., t. 77, 1955, p. 197-217.

[Avril 1957]