SÉMINAIRE N. BOURBAKI

ADRIEN DOUADY

Cohomologie des groupes compacts totalement discontinus

Séminaire N. Bourbaki, 1960, exp. n° 189, p. 287-298

<http://www.numdam.org/item?id=SB_1958-1960__5__287_0>

Séminaire BOURBAKI
12e année, 1959/60, n° 189

Décembre 1959

COHOMOLOGIE DES GROUPES COMPACTS TOTALEMENT DISCONTINUS ([1])

par Adrien DOUADY

[d'après des notes de Serge LANG sur un article non publié de TATE]

1. Groupes compacts totalement discontinus.

Dans cet exposé, $\mathcal{G}$ désignera la catégorie des groupes compacts totalement discontinus (et homomorphismes continus). Ces groupes sont les limites projectives de groupes finis.

EXEMPLE. - Groupe de Galois topologique $G_{E/K}$ d'une extension galoisienne finie ou infinie.

THÉORÈME 1. - Soit G un groupe de $\mathcal{G}$, F et E des sous-groupes fermés de G, tels que $E \subset F$. Alors il existe une section σ continue :

$$G/F \longrightarrow G/E$$

DÉMONSTRATION.

a. Cas où F/E est fini. - Soit H un sous-groupe ouvert distingué de G tel que $H \cap F \subset E$. La projection $\chi : HE/E \to G/F$ est biunivoque, donc bicontinue par compacité ; soit $\sigma : \chi(H) \longrightarrow HE/E$, son inverse, on prolonge σ à G/F en choisissant un représentant dans chaque classe mod H.

b. Cas général On utilise un lemme pour montrer que l'ensemble $\mathcal{E}$ des couples (S, s) où S est un sous-groupe fermé de G tel que $E \subset S \subset F$, et s une section continue :

$$G/F \longrightarrow G/S$$

est inductif.

LEMME 1. - Soit G un groupe compact, S_α une famille filtrante décroissante de sous-groupes fermés de G, $S = \bigcap S_\alpha$. Alors $G/S = \varprojlim G/S_\alpha$.

On se sert de (a.) pour montrer que pour un élément maximal de $\mathcal{E}$, nécessairement $S = E$, ce qui démontre le théorème 1.1.

([1]) Faute de place, les démonstrations ont été réduites au minimum.

DÉFINITION. - On appellera nombre surnaturel une expression formelle $\prod(p^{r_p})$ où p décrit l'ensemble des nombres premiers, les exposants r_p étant des entiers ≥ 0 ou ∞.

On définit de façon naturelle le produit, le plus grand commun dénominateur (pgcd) ou le plus petit commun multiple (ppcm) d'une famille finie ou infinie de nombres surnaturels. On définit l'indice $(G : F)$ d'un sous-groupe fermé F d'un groupe G de $\mathcal{G}$ comme ppcm $(G : V)$ pris sur les sous-groupes V ouverts contenant F.

PROPOSITION 1.1. - Soit G un groupe de $\mathcal{G}$,

a. Si E et F sont des sous-groupes fermés de G, tels que $E \subset F$,

$$(G : E) = (G : F)(F : E)$$

b. Si $F = \bigcap F_\alpha$, (F_α) famille filtrante décroissante de sous-groupes fermés de G,

$$(G : F) = \text{ppcm } (G : F_\alpha)$$

DÉFINITION. - Soit p un nombre premier. On dit que G est un p-groupe de $\mathcal{G}$ si $(G : e)$ est une puissance (finie ou infinie) de p, i. e. si G est limite projective de p-groupes finis. On dit que S est un p-groupe de Sylow d'un groupe G de $\mathcal{G}$ si S est un p-groupe de $\mathcal{G}$ et si $(G : S)$ est premier à p.

THÉORÈME 1.2. de Sylow pour $\mathcal{G}$:

a. Tout p-sous-groupe fermé F d'un groupe G de $\mathcal{G}$ est contenu dans un p-groupe de Sylow.

b. Deux p-groupes de Sylow de G sont conjugués.

DÉMONSTRATION. a. On applique le théorème de Zorn à l'ensemble $\mathcal{E}$ des sous-groupes fermés S de G tels que $(G : S)$ premier à p, ordonné par inclusion décroissante. Pour montrer qu'un S maximal dans $\mathcal{E}$, i. e. minimal pour $\subset$, est un p-groupe, on est ramené au théorème de Sylow pour les groupes finis.

b. Soient S_1 et S_2 deux sous-groupes de Sylow de G. Pour tout sous-groupe ouvert distingué U de G, soit $\chi : G \to G/U$, et K_U l'ensemble des $g \in G$ tels que $\chi(S_2)$ soit conjugué de $\chi(S_1)$ par $\chi(g)$. K_U est un compact non vide et

$$K = \bigcap K_U \neq \emptyset \quad .$$

Tout $g \in K$ transforme S_1 en S_2.

DÉFINITION. - On appelera système de générateurs d'un groupe G de $\mathcal{G}$ une famille (g_i) d'éléments de G telle que :

(SG1) Tout voisinage de e contient tous les g_i sauf un nombre fini d'entre eux.

(SG2) G est le plus petit sous-groupe fermé de G contenant tous les g_i.

THÉORÈME 1.3. - Tout groupe G de $\mathcal{G}$ admet un système de générateurs.

DÉMONSTRATION. - On prend un ensemble d'indice I ayant un cardinal infini strictement plus grand que celui des sous-groupes distingués ouverts de G. Puis on applique le théorème de Zorn à l'ensemble $\mathcal{E}$ des couples $(N, (x_i))$ où N est un sous-groupe distingué fermé de G et (x_i) un système de générateurs de G/N (ce qui entraîne $x_i = e$ pour une infinité de valeurs de i).

DÉFINITION. - Soit (a_i), une famille de lettres, L le groupe libre engendré par les a_i ; on appelle groupe libre de $\mathcal{G}$ (resp. p-groupe libre) engendré par les a_i le groupe $\varprojlim L/V$, pris sur les sous-groupes distingués V de L contenant tous les a_i sauf un nombre fini, et tels que L/V soit fini (resp. fini d'ordre une puissance de p).

EXEMPLE. - Soit C un corps algébriquement clos de caractéristique 0, Ω une clôture algébrique de $C(Z)$. Le groupe de Galois $G_{\Omega/C(Z)}$ est le groupe libre de $\mathcal{G}$ engendré par les éléments de C. [Si $C = \underset{\sim}{C}$, voir l'exposé de Jean-Pierre SERRE ([2])].

Conséquence du théorème 1.3. - Tout groupe de $\mathcal{G}$ est quotient d'un groupe libre, et est un groupe de Galois en caractéristique 0.

2. Modules continus discrets et cohomologie.

Soit G un groupe de $\mathcal{G}$, on notera $\mathfrak{M}(G)$ la catégorie des G-modules A tels que le stabilisateur de tout point a de A soit ouvert, i. e. que l'opération de G sur A, considéré comme discret, soit continue.

EXEMPLES.

1° Soit (G_α) un système projectif de groupes finis, (A_α) un système inductif de groupes abéliens, G_α opérant sur A_α. Pour $\beta < \alpha$, G_α opère sur A_β par l'intermédiaire de G_β, et on suppose que $A_\beta \longrightarrow A_\alpha$ est G_α-linéaire. Posons $G = \varprojlim G_\alpha$ et $A = \varinjlim A_\alpha$. Alors $A \in \mathfrak{M}(G)$.

2° Soit $G_{E/K}$ un groupe de Galois, L une sous-extension normale de E. Alors

---

([2]) "Revêtements ramifiés et groupes discontinus". Exposé fait par Jean-Pierre SERRE pour le chapitre III du Cours de Roger GODEMENT : Fonctions automorphes et théorie des groupes (Faculté des Sciences de Paris, 1958/59, Mathématiques approfondies).

L et L^* sont dans $\mathfrak{M}(G_{E/K})$.

(A) Modules induits.

DÉFINITION. - Soit X un groupe abélien discret, on note $M_G(X)$ le groupe des fonctions continues définies sur G à valeurs dans X , considéré comme G-module par

$$g * \varphi(h) = \varphi(hg) \quad .$$

Un tel module est appelé induit.

C'est un module de $\mathfrak{M}(G)$, et $M_G(X) = \varprojlim X^{G/U}$. On voit, en appliquant le théorème 1.1., que tout module G-induit est aussi F-induit pour tout sous-groupe fermé F de G .

Définissons $\delta : M_G(X) \longrightarrow X$ par $\delta(\varphi) = \varphi(e)$.

PROPOSITION 2.1. - Soit X un groupe abélien, A un module de $\mathfrak{M}(G)$, f , Z-linéaire : $A \longrightarrow X$. Alors il existe une application G-linéaire unique

$$\tilde{f} : A \longrightarrow M_G(X)$$

telle que $\delta \circ f = f$, et $\tilde{f}$ est définie par

$$[\tilde{f}(a)](h) = f(ha) \quad .$$

En prenant pour X le groupe abélien sous-jacent à A et pour f l'identité, on trouve une injection

$$i : A \longrightarrow M_G A \quad .$$

COROLLAIRE. - Tout module A de $\mathfrak{M}(G)$ est sous-module d'un induit.

PROPOSITION 2.2. - Soit X un groupe abélien, A un module de $\mathfrak{M}(G)$, f , G-linéaire : $A \longrightarrow M_G(X)$. Alors f se prolonge en une application G-linéaire

$$M_G(A) \longrightarrow M_G(X) \quad .$$

DÉMONSTRATION. - $\delta \circ f : A \longrightarrow X$ définit une application G-linéaire $\tilde{f} : M_G(\delta \circ f) : M_G(A) \longrightarrow M_G(X)$. On a $\delta \circ \tilde{f} \circ i = \delta \circ f$, d'où $\tilde{f} \circ i = f$ par unicité dans la proposition 2.1.

COROLLAIRE. - Si A est induit, A est un facteur direct de $M_G(A)$.

M_G constitue avec l'injection naturelle i , un foncteur d'effacement exact par des modules induits, la surjectivité à droite étant due à ce que les modules sont discrets.

(B) Cohomologie.

DÉFINITION. - On note $H^0(G , A)$ ou $H^0(A)$ si aucune confusion n'est à craindre, le sous-module de A formé des éléments invariants par G .

Pour tout module A de $\mathfrak{M}(G)$, on considère la suite exacte

$$0 \longrightarrow A \xrightarrow{i} M_G A \longrightarrow A' \longrightarrow 0 \quad ,$$

et on pose

$$H^1(G , A) = H^0(A')/\mathrm{im}\ H^0 M_G A \quad ,$$

et

pour $n \geq 1$. $$H^{n+1}(A) = H^n(A')$$

PROPOSITION 2.3.

a. Les H^n sont des foncteurs additifs ;

b. $H^n(G , A) = 0$ pour $n > 0$ si A est induit ;

c. à toute suite exacte

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

correspond une suite exacte

$$0 \longrightarrow H^0(A) \longrightarrow \ldots \longrightarrow H^n(C) \longrightarrow H^{n+1}(A) \longrightarrow H^{n+1}(B) \longrightarrow \ldots \quad .$$

REMARQUE. - Il y a assez d'injectifs dans la catégorie $\mathfrak{M}(G)$, car, si Q est un G-module injectif, le sous-module Q^0 de Q, formé des éléments dont le stabilisateur est ouvert, est injectif dans $\mathfrak{M}(G)$. En effet, tout G-homomorphisme d'un module de $\mathfrak{M}(G)$ dans Q prende ses valeurs dans Q^0. Tout injectif est facteur direct d'un induit, et H^k (resp. H^{i+k}) est le k-ième dérivé (resp. satellite) droit de H^0 (resp. H^i) pour $k \geq 0$, $i \geq 0$. En particulier $H^n(G , A) = \mathrm{Ext}^n_G(Z , A)$. Par contre, si G est infini, il n'y a pas de projectif autre que 0 dans $\mathfrak{M}(G)$.

(C) Calcul par cochaînes.

A tout module A de $\mathfrak{M}(G)$, associons la suite exacte

$$0 \longrightarrow A \xrightarrow{\varepsilon} C^0 \xrightarrow{d} C^1 \longrightarrow \ldots$$

où C^n est le groupe des applications continues γ de G^{n+1} dans A, muni de la multiplication $(g\gamma)(x_0 , x_1 , \ldots , x_n) = g_0 \gamma(g_0^{-1} x_0 , \ldots , g^{-1} x_n)$, l'application $d : C^n \longrightarrow C^{n+1}$ étant définie par

$$d\gamma(x_0 , \ldots , x_{n+1}) = \sum (-1)^i \gamma(x_0 , \ldots , \hat{x}_i , \ldots , x_{n+1}) \quad ,$$

et ε par $\varepsilon(a)$ = fonction constante a. Les modules C^n sont induits, et $H^*(G , A)$ est l'homologie du complexe

$$0 \longrightarrow H^0(G , C^0) \longrightarrow H^0(G , C^1) \longrightarrow \ldots$$

Le groupe $H^1(G , A)$ s'identifie au groupe des homomorphismes croisés continus

de G dans A et, si A est fini, $H^2(G , A)$ s'identifie à l'ensemble des classes d'extension $0 \to A \to E \to G$ où $E \in \mathcal{G}$ (utiliser le théorème 1.1.).

(D) Changement de groupe.

Soit $A \in \mathfrak{M}(G)$. À un homomorphisme continu $\varphi : G' \to G$ correspond

$$\varphi^* : H^*(G , A) \to H^*(G' , A) \quad .$$

En particulier :

lift : $H^*(G/N , B) \to H^*(G , B)$ pour N fermé distingué dans G et $B \in \mathfrak{M}(G/N)$

res : $H^*(G , A) \to H^*(F , A)$ pour F fermé dans G et $A \in \mathfrak{M}(G)$.

Soit maintenant V un sous-groupe ouvert de G , on définit :

cores : $H^*(V , A) \to H^*(G , A)$ pour $A \in \mathfrak{M}(G)$

cores o res : $H^*(G , A) \to H^*(G , A)$ coïncide avec la multiplication par $(G : V)$.

THÉORÈME 2.1. - $H^*(G , A) = \varinjlim H^*(G/U , H^0(U , A))$.

Plus généralement, si $G = \varprojlim G_\alpha$, $A = \varinjlim A_\alpha$, avec $A_\alpha \in \mathfrak{M}(G_\alpha)$ et pour $\beta < \alpha$, $A_\beta \to A_\alpha$ est G_α-linéaire ; alors :

$$H^*(G , A) = \varinjlim H^*(G_\alpha , A_\alpha) \quad .$$

DÉMONSTRATION. - On montre que $C^n(G , A) = \varinjlim C^n(G_\alpha , A_\alpha)$.

COROLLAIRE 1. - Les $H^n(G , A)$ sont de torsion pour $n > 0$.

COROLLAIRE 2. - Si F est un sous-groupe fermé de G et $(G : F)$ premier à p , res : $H^*(G , A) \to H^*(F , A)$ est injective sur la partie p-primaire.

(E) Modules relativement induits.

Soit $F \subset G$ et $B \in \mathfrak{M}(F)$. On note $M_G^F(B)$ le sous-module de $M_G(B)$ formé des φ telles que $f\varphi(x) = \varphi(fx)$ pour tout $f \in F$.

PROPRIÉTÉS.

a. M_G^F est un foncteur exact.

b. Si $A \in \mathfrak{M}(G)$, $\mathrm{Hom}_G(A , M_G^F(B)) = \mathrm{Hom}_F(A , B)$.

c. $M_G^F(B) = \varinjlim M_{G/U}^{F/U \cap F}(H^0(F \cap U , B))$.

d. $H^*(G , M_G^F(B)) = H^*(F , B)$, comme on le voit en remarquant que, si B est F-induit, $M_G^F(B)$ est G-induit, car $M_G(X) = M_G^F(M_F(X))$.

(F) Suites spectrales.

THÉORÈME 2.2. - Soit N fermé distingué dans G et $A \in \mathfrak{M}(G)$. Alors on a une suite spectrale dont le terme E_2 est $H^*(G/N , H^*(N , A))$ et dont le terme E_∞

est le gradué associé à $H^*(G , A)$ convenablement filtré. De plus

$$\text{res} : H^*(G , A) \longrightarrow H^*(N , A)$$

et

$$\text{lift} : H^*(G/N , H^0(N , A)) \longrightarrow H^*(G , A)$$

sont les homomorphismes latéraux.

DÉMONSTRATION. - Connue dans le cas fini, elle s'obtient dans le cas infini par passage à la limite inductive grâce au théorème 2.1.

3. Dimension cohomologique.

DÉFINITION. - Soit $G \in \mathcal{C}$ et p premier. On définit la dimension cohomologique cd_p (resp. la dimension cohomologique stricte scd_p) relative à p par

$cd_p(G) \leq n \Longleftrightarrow$ partie p-primaire de $H^r(G , A) = 0$ pour $r > n$ et $A \in \mathfrak{M}(G)$ de torsion.

$scd_p(G) \leq n \Longleftrightarrow$ partie p-primaire de $H^r(G , A) = 0$ pour $r > n$ et $A \in \mathfrak{M}(G)$.

$cd(G) = \sup cd_p(G)$

$scd(G) = \sup scd_p(G)$

PROPOSITION 3.1. - $cd_p(G) \leq scd_p(G) \leq cd_p(G) + 1$.

DÉMONSTRATION. - La première inégalité est triviale.
Soit $A \in \mathfrak{M}(G)$ et $r > cd_p(G)$. Les suites exactes :

$$0 \to pA \xrightarrow{i} A \to A_p \to 0$$

$$0 \to {}_pA \to A \xrightarrow{p} pA \to 0$$

donnent

$$\begin{array}{ccccc} H^{r+1}({}_pA) & \to & H^{r+1}(A) & \xrightarrow{p_*} & H^{r+1}(pA) \\ \| & & & & \\ H^r(A_p) & \longrightarrow & H^{r+1}(pA) & \xrightarrow{i_*} & H^{r+1}(A) \end{array}$$

d'où $p = i_* \circ p_*$: $H^{r+1}(A) \to H^{r+1}(A)$ est injective, i. e. $H^{r+1}(A)$ n'a pas de p-torsion.

PROPOSITION 3.2.

a. Si $F \subset G$ fermé, $cd_p(F) \leq cd_p(G)$

b. Si de plus $(G : F)$ premier à p , $cd_p(F) = cd_p(G)$

En particulier si G_p est un p-groupe de Sylow de G ;

$$cd(G_p) = cd_p(G_p) = cd_p(G) \quad .$$

DÉMONSTRATION.

a. Voir paragraphe 2, (E), propriété (d) ;

b. Corollaire 2 du théorème 2.1.

THÉORÈME 3.1. - Si G est un p-groupe de $\mathcal{G}$, $cd(G) \leqslant n$ si, et seulement si $H^{n+1}(G , Z_p) = 0$.

DÉMONSTRATION. - On montre que $H^{n+1}(G , A) = 0$, successivement :

a. Pour tout module fini A d'ordre une puissance de p (suite de composition)

b. Pour tout module fini (somme directe de ses composantes q-primaires)

c. Pour tout module de torsion ($\varinjlim$ des précédents)

d'où $H^{n+1}(G , \ ) = 0$, et ses foncteurs satellites droits $H^{n+k+1}(G , \ )$ sont aussi nuls, car le foncteur M_G ne fait pas sortir de la catégorie exacte des modules de torsion.

THÉORÈME 3.2. - Soit G un p-groupe de $\mathcal{G}$, tel que $cd(G) = n$ fini. Alors $H^n(G , A) \neq 0$ pour tout module fini non nul $A \in \mathcal{M}(G)$ d'ordre une puissance de p .

DÉMONSTRATION. - Soit A' un sous-module de A tel que $A/A' = Z_p$. La suite exacte

$$H^n(G , A) \longrightarrow H^n(G , Z_p) \longrightarrow \underset{\| \, 0}{H^{n+1}}(G , A')$$

montre que $H^n(G , A) = 0 \Rightarrow H^n(G , Z_p) = 0$ contrairement au théorème 3.1.

COROLLAIRE. - Soit V ouvert dans G . Si $cd_p(G) = n$ fini, $cd_p(V) = n$.

DÉMONSTRATION. - On sait que $cd_p(V) \leqslant n$.

a. Si G est un p-groupe,

$$H^n(V , Z_p) = H^n(G , M_G^V(Z_p)) \neq 0$$

par le théorème 3.2.

b. Si G est quelconque : soit V_p un p-groupe de Sylow de V , G_p un p-groupe de Sylow de G le contenant :

$$cd_p(G) = cd_p(G_p) = cd_p(V_p) = cd_p(V) \quad .$$

THÉORÈME 3.3.

a. $cd(G) = 0$ si, et seulement si $G = \{e\}$

b. $cd_p(G) \leqslant 1$ si et seulement si G est p-extensif, i. e. si pour tout $F \in G$, pour tout $E \subset F$ fermé distingué, tout homomorphisme continu $G \longrightarrow F/E$ se relève en G un homomorphisme continu $G \longrightarrow F$.

c. Si $cd_p(G) = 1$, $scd_p(G) = 2$.

DÉMONSTRATION.

a. Si $cd(G) = 0$, $cd(G_p) = 0$, $H^1(G_p, Z_p) = 0$, $G_p = \{e\}$ pour tout p, d'où $G = \{e\}$

c. $scd_p(G) = 1$ ou 2. Si $scd_p(G) = 1$, $scd(G_p) = 1$, $H^1(G_p, Q/Z) = H^2(G_p, Z) = 0$, $G_p = \{e\}$ et $scd_p(G) = scd(G_p) = 0$ absurde.

b. La condition est suffisante, car elle entraîne que toute extension de G par E fini d'ordre une puissance de p est un produit croisé, d'où $H^2(G, E) = 0$ pour tout E, et $cd_p(G) \leqslant 1$. Montrons qu'elle est nécessaire.

Cas où E est fini. - Soit Γ l'extension de G par E image réciproque de l'extension F de F/E.

$$\begin{array}{ccc} \Gamma & \xrightarrow{\bar{f}} & F \\ \downarrow & & \downarrow \\ G & \xrightarrow{f} & F/E \end{array}$$

Il existe un homomorphisme $\sigma : G \longrightarrow \Gamma$, car la classe de Γ dans $H^2(G, E)$ est nulle, et $\bar{f} \circ \sigma$ répond à la question.

Cas où E est infini.- On applique le théorème de Zorn à l'ensemble $\mathcal{E}$ des couples (H, h) où H est un sous-groupe distingué fermé de F contenu dans E, et $h : G \longrightarrow F/H$ un homomorphisme continu relevant f.

PROPOSITION 3.3. - Soit G un p-groupe de $\mathcal{C}$. Pour que $cd(G) \leqslant 1$, il faut et il suffit que G soit p-libre.

DÉMONSTRATION. - Tout p-groupe libre est p-extensif, donc a $cd \leqslant 1$. Soit G^*, l'intersection des noyaux des homomorphismes continus $G \longrightarrow Z_p$. $H^1(G, Z_p)$ et G/G^* sont en dualité de Pontrjagin. Soit B une base de $H^1(G, Z_p)$, L le p-groupe libre engendré par B. On a

$$L/L^* = Z_p^B = G/G^* \quad .$$

L'homomorphisme $\omega : L \longrightarrow G/G^*$ se relève en $\omega : L \longrightarrow G$.
Comme la première est sur, la seconde aussi (par un lemme de Nakayama qui s'étend à $\mathcal{C}$). Si $cd(G) \leqslant 1$, il existe $\sigma : G \longrightarrow L$ telle que $\omega \circ \sigma = I_G$, donc σ biunivoque. D'autre part σ est sur, car $G \longrightarrow L/L^*$ l'est. D'où la proposition 3.3.

PROPOSITION 3.4. - Soit G un groupe de $\mathcal{G}$, $G(p)$ son plus gros p-quotient, i. e. son quotient par l'intersection des noyaux de ses homomorphismes dans des p-groupes. Alors si $H^2(G, Z_p) = 0$, $cd(G(p)) \leq 1$.

THÉORÈME 3.4. (de la tour) : Si $N \subset G$ fermé distingué,

$$cd_p(G) \leq cd_p(G/N) + cd_p(N)$$

DÉMONSTRATION. - Voir le théorème 2.2.

4. Applications à la théorie de Galois.

THÉORÈME 4.1. - Soit k un corps de caractéristique $p \neq 0$, $k(p)$ sa plus grande p-extension séparable. Son groupe de Galois $G(p) = G_{k(p)/k}$ est un p-groupe libre, engendré par une base du Z_p-espace vectoriel $k/\wp(k)$, où $\wp : k \longrightarrow k$ désigne la fonction de Kummer : $\wp(x) = x - x^p$.

DÉMONSTRATION. - Il suffit (proposition 3.3. et théorème 3.1.) de montrer que

$$H^2(G(p), Z_p) = 0$$

et

$$H^1(G(p), Z_p) = k/\wp k \quad .$$

On le voit par la suite exacte

$$0 \longrightarrow Z_p \longrightarrow k(p) \xrightarrow{\wp} k(p) \longrightarrow 0 \quad ,$$

en tenant compte de $H^0(G(p), k(p)) = k$ et $H^i(G(p), k(p)) = 0$ pour $i > 0$.

COROLLAIRE. - Soit $G_k = G_{k_s/k}$ le groupe de Galois de la clôture séparable de k. Alors $cd_p G_k \leq 1$.

DÉMONSTRATION. - Soit G_p un p-groupe de Sylow de G_k, k_p son corps des invariants, on a $G_p = G_{k_p}$, d'où $cd_p G_k = cd G_p \leq 1$.

PROPOSITION 4.1. - Soit k un corps de caractéristique $q \neq p$, contenant les racines p-ièmes de 1, $k(p)$ sa plus grande p-extension séparable, $G(p)$ son groupe de Galois. Alors $cd(G(p)) \leq n$ si et seulement si :

$$\begin{cases} H^n(G(p), k(p)^*) \text{ divisible par } p \\ H^{n+1}(G(p), k(p)^*) = 0 \end{cases} .$$

DÉMONSTRATION. - On utilise la suite exacte

$$0 \longrightarrow Z_p \longrightarrow k(p)^* \xrightarrow{p} k(p)^* \longrightarrow 0 \quad .$$

PROPOSITION 4.2. - Si le groupe de Brauer $H^2(G_k , k_s^*) = 0$, $G(p)$ est un p-groupe libre.

DÉMONSTRATION. - La suite exacte

$$0 \longrightarrow Z_p \longrightarrow k_s^* \xrightarrow{p} k_s^* \longrightarrow 0$$

et Hilbert 90 donnent : $H^2(G_k , Z_p) = 0$. On applique les propositions 3.4. et 3.3.

THÉORÈME 4.2. - Soit k un corps non séparablement clos, et supposons que toute extension séparable finie K de k ait son groupe de Brauer $H^2(G_K , k_s^*) = 0$. Alors $cdG_k = 1$.

DÉMONSTRATION. - Soit G_p un groupe de Sylow de G_k . On a $G_p = \cap G_K$ pour les extensions K finies contenues dans k_p , d'où $H^2(G_p , k_s^*) = 0$ par le théorème 2.1. On a $cd_p\ G = cdG_p \leqslant 1$ par la proposition 4.2. pour $p \neq$ car. k et par le théorème 4.1. pour $p =$ car. k .

APPLICATIONS. - Si k est un corps p-adique , $cdG_k = 2$.

DÉMONSTRATION. - Soit L la plus grande extension non ramifiée de k . $G_{L/k} = G_{Z_p}$ est libre à 1 générateur, donc $cdG_{L/k} = 1$. D'autre part, toute extension finie K de L , n'a pas d'extension non ramifiée autre qu'elle-même, donc $H^2(G_K , k_s^*) = 0$ ([3]) et $cdG_L \leqslant 1$ par le théorème 4.2. Enfin $cdG_k \leqslant 2$ par le théorème 4.4. de la tour.

THÉORÈME 4.3. - Si K est une extension de type fini de k , et $cd_p(G_k) = n$ fini, on a

$$cd_p(G_K) = cd_p(G_k) + tr.\ d^\circ(K/k)$$

DÉMONSTRATION. - On est ramené aux cas particuliers suivants :

a. Extension finie : voir corollaire du théorème 3.2.

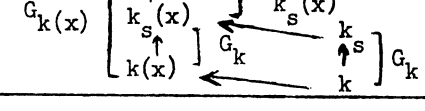
b. Extension $k(x)$: on a $G_{k_s/k(x)} = G_{k_s/k} = G_k$.

D'autre part $cdG_{k_s(x)} = 1$ par le théorème 4.2. et le théorème de Tsen.

D'où $cd_p\ G_{k(x)} \leqslant cd_p\ G_k + 1$

par le théorème 3.4. de la tour.

Montrons qu'on a l'égalité :



([3]) Cf. p. III-27 de Jean-Pierre SERRE : Homologie des groupes, applications arithmétiques, Cours professé au Collège de France, 1958/59, multigraphié. Voir aussi Serge LANG : On quasi algebraic closure, Annals of Math., t. 55, 1952, p. 373-390 (Thèse Ph. D., Princeton University, 1951).

Cas où G_k est un p-groupe. - La suite spectrale (théorème 2.2.) donne

$$H^{n+1}(G_{k(x)}\ ,\ Z_p) = H^n(G_k\ ,\ H^1(G_{k_s(x)}\ ,\ Z_p))\quad .$$

Mais $H^1(G_{k_s(x)}\ ,\ Z_p)$ contient Z_p comme facteur direct de G_k-module, donc

$$H^{n+1}(G_{k(x)}\ ,\ Z_p) \neq 0\quad .$$

Cas où G_k est quelconque. - On utilise un p-groupe de Sylow G_p de G_k et son corps k_p : $cd_p(G_{k(x)}) \geqslant cd_p(G_{k_p(x)}) = cd(G_p) + 1 = cd_p(G_k) + 1$.

D'où le théorème 4.3.

REMARQUE. - Pour $p = car.\ k$, voir corollaire du théorème 4.1. Sans l'hypothèse de type fini, on a

$$cd_p\ G_K \leqslant cd_p\ G_k + tr.\ d°(K/k)$$

Ce théorème est, en fait, à l'origine de la théorie, sa conjecture et le schéma de sa démontration étant dûs à GROTHENDIECK.