Pierre Samuel

Théorie du corps de classes local selon G. P. Hochschild

Séminaire N. Bourbaki, 1952, exp. nº 42, p. 349-353
<http://www.numdam.org/item?id=SB_1948-1951__1__349_0>

Séminaire BOURBAKI
(Mars 1951)

THÉORIE DU CORPS DE CLASSES LOCAL SELON G.P. HOCHSCHILD ([1]).

par Pierre SAMUEL

1. Enoncé des résultats.

Soit K un corps $\mathfrak{p}$-adique. Pour toute extension abélienne finie L de K, $N_{L/K}(L^*)$ est un sous-groupe d'indice fini de K^* de groupe quotient $N^*/N(L^*)$ isomorphe au groupe de Galois $\mathfrak{G}$ de L. Tout sous-groupe d'indice fini de K^* est de la forme $N_{L/K}(L^*)$ où L est une extension abélienne finie. Si F est une extension finie quelconque de K et si R est la plus grande extension abélienne contenue dans F, on a $N_{R/K}(R^*) = N_{F/K}(F^*)$.

2. Cohomologie des groupes de Galois.

Soient L une extension galoisienne d'un corps (quelconque) K, $\mathfrak{G}$ son groupe de Galois. Le groupe abélien $C^n(\mathfrak{G}, L^*)$ des applications de $\mathfrak{G}^n$ dans L^* est appelé le groupe des cochaînes de d^{0}n ($C^0 = L$). Opérateur de cobord défini par

$$\delta f(\sigma_1, \dots, \sigma_{n+1}) =$$
$$f(\sigma_2, \dots, \sigma_{n+1})^{\sigma_1} \prod_i f(\sigma_1, \dots, \sigma_i\sigma_{i+1}, \dots \sigma_{n+1})^{(-1)^i} f(\sigma_1, \dots, \sigma_n)^{(-1)^{n+1}}$$

pour $f \in C^n$; on vérifie que $\delta\delta f = 1$; cas particuliers utiles :

1° $n = 0$, $f \in L^*$, $(\delta f)(\sigma) = f^\sigma f^{-1}$.

2° $n = 1$, $(\delta f)(\sigma, \tau) = f(\tau)^\sigma f(\sigma\tau)^{-1} f(\sigma)$.

3° $n = 2$, $(\delta f)(\sigma_1, \sigma_2, \sigma_3) = f(\sigma_2, \sigma_3)^{\sigma_1} f(\sigma_1\sigma_2, \sigma_3)^{-1} f(\sigma_1, \sigma_2\sigma_3) f(\sigma_1, \sigma_2)^{-1}$

On définit alors cocycles, cobords et groupes de cohomologie $H^n(\mathfrak{G}, L^*)$ (H^2 est le groupe des classes d'algèbres centrales simples sur K qui sont décomposées par L).

a. On montre (par l'indépendance linéaire des automorphismes) que $H^1 = (1)$. Soit $\mathfrak{H}$ un sous-groupe invariant de $\mathfrak{G}$, F son corps des invariants, $\mathfrak{G}/\mathfrak{H}$

([1]) HOCHSCHILD (G.). - Local class field theory, Annals of Math., Series 2, t. 51, 1950, p. 331-347.

le groupe de Galois de F sur K ; on a les applications canoniques

$$C^n(\mathfrak{G}/\mathfrak{H}, F^*) \to C^n(\mathfrak{G}, L^*) \to C^n(\mathfrak{H}, L^*),$$

qui passent à la cohomologie et donnent la suite suivante, qu'on démontre être exacte :

$$(1) \qquad \to H^2(\mathfrak{G}/\mathfrak{H}, F^*) \xrightarrow[\tau_{F,L}]{} H^2(\mathfrak{G}, L^*) \to H^2(\mathfrak{H}, L^*)$$

(que SERRE sait faire aller plus loin). Si $\mathfrak{H}$ est d'ordre m, et si $c \in H^2(\mathfrak{G}, L^*)$ on voit par "moyenne sur $\mathfrak{H}$" que c^m est dans le noyau du dernier homomorphisme, et donc dans l'image de $\tau_{F,L}$.

b. On suppose maintenant que toutes les extensions de K considérées sont plongées dans une même clôture algébrique ; ce plongement est unique pour les galoisiennes. Soient E, F deux extensions galoisiennes de K, C leur (unique) extension composée, qui est galoisienne, de groupe $\mathfrak{C}$; soient $\mathfrak{C}_E$, $\mathfrak{C}_F$ les sous-groupes invariants des éléments de $\mathfrak{C}$ qui laissent E, F invariants ; les groupes de Galois $\mathfrak{E}, \mathfrak{F}$ de E, F sont $\mathfrak{C}/\mathfrak{C}_E, \mathfrak{C}/\mathfrak{C}_F$. Considérons les isomorphismes $\tau_{E,C}$, $\tau_{F,C}$ de $H^2(\mathfrak{E}, E^*)$, $H^2(\mathfrak{F}, F^*)$ dans $H^2(\mathfrak{C}, C^*)$; à l'intersection de leurs images dans $H^2(\mathfrak{C}, C^*)$ correspondent deux sous-groupes $H^2(\mathfrak{E}, E^*)_F$ et $H^2(\mathfrak{F}, F^*)_E$ isomorphes par des isomorphismes réciproques notés $\tau_{E,F}$ et $\tau_{F,E}$; ceux-ci vérifie une propriété évidente de transitivité.

c. ("L'homomorphisme japonais") Soit $c \in H^2(\mathfrak{G}, L^*)$; pour tout représentant f de c dans Z^2, on pose $\bar{f}(\sigma) = \prod_{\tau \in \mathfrak{G}} f(\tau, \sigma)$; en faisant les produits en σ_1 et en σ_2 des formules 3° du cobord, on obtient

$$1 = N(f(\sigma, \tau))\bar{f}(\tau)^{-1}\bar{f}(\sigma\tau)\bar{f}(\sigma)^{-1} \quad \text{et} \quad \bar{f}(\sigma)^{\mu} = \bar{f}(\sigma).$$

Donc $\bar{f}$ définit un homomorphisme de $\mathfrak{G}$ dans $K^*/N(L^*)$; on vérifie aisément qu'il ne dépend que de la classe de cohomologie c de f, et on le note c' ; ainsi $c \to c'$ est un homomorphisme : $H^2(\mathfrak{G}, L^*) \to \mathrm{Hom}(\mathfrak{G}, K^*/N(L^*))$.

Soit F une sous-extension de L, galoisienne sur K ; considérons les homomorphismes :

$$H^2(\mathfrak{G}/\mathfrak{H}, F^*) \xrightarrow[\tau_{F,L}]{} H^2(\mathfrak{G}, L^*) \to H^2(\mathfrak{H}, L^*)$$

(où $\mathfrak{G}/\mathfrak{H}$ est le groupe de Galois de F) (cf.a)) ; on démontre qu'on a le diagramme de compatibilité suivant :

(c)'
$$\begin{tikzcd} \mathfrak{H} \arrow[r] \arrow[d] & \mathfrak{G} \arrow[r] \arrow[d, "c'"'] & \mathfrak{G}/\mathfrak{H} = \mathfrak{F} \arrow[d, "(\mu_{L,F}(c))'"] \\ F^*/N_{L/F}(L^*) \arrow[r, "\bar{N}"'] & K^*/N(L^*) \arrow[r] & K^*/N(F^*) \end{tikzcd}$$

où $c \in H^2(\mathfrak{G}, L^*)$, et où $\bar{N}$ se déduit de $N_{F/K}$ par passage aux quotients ; la moitié gauche est encore valable pour une sous-extension quelconque F de L ; enfin $\mu_{L,F}(c)$ est défini ainsi : si $m = [L : F]$, c^m est de la forme $\tau_{F,L}(e)$ (a)), et l'on peut poser $e = \mu_{L,F}(c)$ puisque $\tau_{F,L}$ est biunivoque.

(α) On montre enfin que, si L est cyclique sur K , $c \to c'$ est un isomorphisme de $H^2(\mathfrak{G}, L^*)$ sur $\mathrm{Hom}(\mathfrak{G}, K^*/N(L^*))$ (prendre un cocycle convenablement normalisé dans la classe c).

3. Définition de l'homomorphisme principal.

Soit K un corps valué par une valuation discrète v , complet, et tel que le corps des valeurs de v soit fini (K est soit un corps $\mathfrak{p}$-adique, soit un corps de séries formelles à une variable sur un corps fini) ; nous noterons A_K et P_K l'anneau et l'idéal de v , I_K l'ensemble des éléments inversibles de A_K . Toute extension finie L de K a les mêmes propriétés ; on pose

$$f = [A_L/P_L : A_K/P_K] \quad , \text{ et } \quad P_K A_L = (P_L)^{\epsilon} \; ;$$

alors $[L : K] = ef$. Si L est galoisienne tout $\sigma \in \mathfrak{G}$ est continu (unicité de la valuation de L) ; les automorphismes $\sigma \in \mathfrak{G}$ tels que $a^{\sigma} - a \in P_L$ pour tout $a \in A_L$ forment un sous-groupe invariant $\mathfrak{T}$ de $\mathfrak{G}$; appelé le sous-groupe d'inertie de L ; $\mathfrak{T}/\mathfrak{G}$ est le groupe de Galois de A_L/P_L sur A_K/P_K , et est donc cyclique ; le corps des invariants de $\mathfrak{T}$ est le corps d'inertie T ; on a

$$[T : K] = f \; , \; [L : T] = e \; .$$

Si $e = 1$, L est dite non ramifiée. Il existe des extensions non ramifiées de $d^0 n$ de K (relever une équation irréductible $f(X)$ de $d^0 n$ sur A_K/P_K) ; deux telles extensions sont identiques (appliquer le lemme de Hensel à $f(X)$) ; une extension non ramifiée L de K est galoisienne (encore HENSEL), et son groupe de Galois est cyclique (ici = (1)) ; si q est le nombre d'éléments de A_K/P_K , l'automorphisme de L qui, dans A_L/P_L donne $x \to x^q$, est appelé l'automorphisme de Frobenius.

Si Z est l'extension non ramifiée de $d^0 n$ de K , $N(Z^*)$ est l'ensemble V des

$x \in K^*$ tels que $n|v(x)$ (il suffit de montrer que tout élément de I_K est une norme, ce qui se fait par approximations successives en utilisant le fait que tout élément d'un corps fini est une norme et une trace). Ainsi $K^*/N(Z^*)$ est un groupe cyclique d'ordre n, engendré par la classe $\overline{\pi}$ des générateurs de P_K. On définit alors $\varphi_{Z/K} : \mathfrak{Z} \to K^*/N(Z^*)$ par $\varphi_{Z/K}$ (Frobenius) $= \overline{\pi}$; en vertu de (α) (paragraphe 2) il existe un c et un seul dans $H^2(\mathfrak{Z}, Z^*)$ tel que $\varphi_{Z/K} = c'$. On montre alors le résultat suivant :

(β) <u>Si</u> F <u>est galoisienne de</u> $d^0 n$ <u>sur</u> K, <u>et si</u> Z <u>désigne l'extension non ramifiée de</u> $d^0 n$ <u>de</u> K, <u>alors</u> $\tau_{Z,F}$ (2,b)) <u>est partout définie</u> sur $H^2(\mathfrak{Z}, Z^*)$ (on considère l'extension composée U de Z et F, et on montre que $\tau_{Z,U}(c)$ est dans le noyau de $H^2(\mathfrak{U}, U^*)$ $H^2(\mathfrak{U}_F, \mathfrak{U}^*)$). L'élément $\tau_{Z,F}(c) \in H^2(\mathfrak{F}, F^*)$ est appelé la <u>classe principale de cohomologie</u> de F, et $(\tau_{Z,F}(c))'$ <u>l'homomorphisme principal</u> de F ; on le note $\varphi_{F/K}$. Si F est une sous-extension galoisienne de l'extension galoisienne L de K, on a le diagramme de compatibilité suivant (dont la partie gauche est valable pour une sous-extension quelconque F) :

$$\begin{array}{ccccc}
\mathfrak{L}_F & \longrightarrow & \mathfrak{L} & \longrightarrow & \mathfrak{L}/\mathfrak{L}_F \\
\varphi_{L/F}\downarrow & & \varphi_{L/K}\downarrow & & \varphi_{F/K}\downarrow \\
F^*/N_{L/F}(L^*) & \xrightarrow{\overline{N}} & K^*/N_{L/K}(L^*) & \longrightarrow & K^*/N_{F/K}(F^*)
\end{array}$$

(il suffit de vérifier que les $\overline{\pi}$ et les Frobenius des diverses extensions non ramfiées utilisées dans les constructions des φ se comportent comme il faut). Si L est galoisienne et F algébrique finie quelconque et si U désigne leur extension composée, ce diagamme se généralise en :

$$\begin{array}{ccccc}
\mathfrak{U}_F & \longrightarrow & & & \mathfrak{L} \\
\varphi_{U/F}\downarrow & & & & \varphi_{L/K}\downarrow \\
F^*/N_{U/F}(U^*) & \xrightarrow{N} & K^*/N_{U/K}(U^*) & \longrightarrow & K^*/N_{L/K}(L^*)\ .
\end{array}$$

4. <u>Les théorèmes principaux.</u>

On fait intervenir ici le seul résultat arithmétique un peu profond de la théorie : <u>si</u> L <u>est une extension cyclique du corps</u> $\mathfrak{p}$<u>-adique</u> K, <u>on a</u> $(K^* : N(L^*)) = [L:K]'$ (Démonstration dans la thèse de Chevalley, au moyen du lemme d'Herbrand, de l'exponentielle $\mathfrak{p}$-adique et du théorème normique de Hilbert), pour nos besoins il suffirait d'avoir l'inégalité " $\leqslant$ ", qui se démontre facilement dans le cas où le nombre de ramification e de L n'est pas multiple de p).

Alors $H^2(\mathfrak{L}, L^*)$ a même ordre que $(K^* : N(L^*))((\alpha)$ (paragraphe 2); soit Z

l'extension non ramifiée de $d^0 [L : K]$ de K ; comme $\mathcal{T}_{Z,F}$ applique isomorphiquement $H^2(\mathfrak{Z}, Z^*)$ dans $H^2(\mathfrak{L}, L^*)((\beta)$, par. 3), c'est une application sur, et $\varphi_{L/K}$ est un isomorphisme de $\mathfrak{L}$ sur $K^*/N(L^*)$.

De là, et des diagrammes du paragraphe 3, on déduit que si U est l'extension composée de L galoisienne et de C cyclique, on a $N(U^*) = N(L^*) \cap N(C^*)$. D'où, en considérant une extension abélienne de K comme composée d'extensions cycliques linéairement disjointes (groupes abéliens finis) et en regardant les diagrammes :

THÉORÈME 1. - Si L est une extension abélienne d'un corps $\mathfrak{p}$-adique K, $\varphi_{L/K}$ est un isomorphisme du groupe de Galois de L sur $K^*/N_{L/K}(L^*)$.

Pour le second théorème annoncé en 1 , on remarque d'abord que

$$N_{L/K}(L^*) \subset N_{M/K}(M^*)$$

entraîne $L \subset M$ pour des extensions abéliennes L et M (extension composée et diagrammes), et qu'à tout sous-groupe H tel que $N_{L/K}(L^*) \subset H \subset K$ correspond une sous-extension F de L telle que $H = N_{F/K}(F^*)$ (considérer le sous-groupe de $\mathfrak{L}$ correspondant à H). Soit maitenant H un sous-groupe quelconque d'indice fini de K ; comme $H \supset K^{*n}$, il suffit de montrer que K^{*n} est un groupe de normes ce qui est relativement facile lorsque K contient les racines n-ièmes de l'unité (que K^{*n} soit l'indice fini résulte par exemple de la fonction exponentielle ; alors, par adjonction à K de toutes les racines n-ièmes d'éléments de K, on obtient une extension abélienne finie L, de degré $(K^* : K^{*n})$ et composée d'extensions cycliques de degrés diviseurs de n ; d'où $K^{*n} = N_{L/K}(L^*)$).. Sinon l'on adjoint à K les racines n-ièmes de l'unité, soit R le corps obtenu, et on "redescend" de R à K par une chaîne d'extensions cycliques. D'où :

THÉORÈME 2. - Soit K un corps $\mathfrak{p}$-adique ; pour tout sous-groupe d'indice fini H de K, il existe une extension abélienne telle que $H = N(L^*)$.

Soit enfin F une extension finie quelconque de K. D'après le théorème 2, il existe une extension abélienne L telle que $N_{L/K}(L^*) = N_{F/K}(F^*)$. Si U est l'extension composée de L et F, le dernier diagramme du paragraphe 3 montre que $L \subset F$. Il est clair que L est la plus grande sous-extension abélienne de F ; c'est le corps des invariants du groupe des commutateurs $\mathfrak{C}$ du groupe de Galois $\mathfrak{F}$ de F lorsque F est galoisienne, et on a $\varphi_{L/K} = \varphi_{F/K} \circ \pi (\pi : \mathfrak{F} \to \mathfrak{F}/\mathfrak{C})$.