SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Corps locaux et isogénies

Séminaire N. Bourbaki, 1958-1960, exp. n° 185, p. 239-247

<http://www.numdam.org/item?id=SB_1958-1960__5__239_0>

Séminaire BOURBAKI
(Mai 1959)

CORPS LOCAUX ET ISOGÉNIES

par Jean-Pierre SERRE

On sait que l'on peut associer à toute variété algébrique V un système projectif de groupes algébriques commutatifs de telle sorte que tout revêtement abélien de V soit image réciproque d'une isogénie d'un de ces groupes. Lorsque V est une courbe définie sur un corps fini k, ce résultat, joint à la détermination des k-isogénies, conduit tout de suite aux théorèmes dits "du corps de classes". C'est la méthode de LANG ([5], voir aussi [6], Chap. VI).

Nous allons voir que la même méthode s'applique au cas local (et aussi bien en inégale caractéristique) : si K est un corps complet pour une valuation discrète, et de corps des restes k algébriquement clos, les extensions abéliennes de K correspondent biunivoquement aux isogénies du groupe des unités de K, ce dernier groupe étant considéré comme limite projective de k-groupes algébriques (cf. n° 4, théorème 2). Le cas d'un corps des restes fini ("corps de classes local") se ramène facilement au précédent (cf. n° 7).

1. Structure de groupe algébrique sur le groupe des unités.

[Les résultats résumés ci-dessous sont dus à M. GREENBERG (non publié)].

Soit d'abord M un anneau d'Artin local, de corps des restes k algébriquement clos ; si k est de caractéristique zéro, on choisit un relèvement $k \longrightarrow M$, et M devient un espace vectoriel de dimension finie sur k, donc se trouve muni automatiquement d'une structure de variété algébrique sur k. Si k est de caractéristique $p \neq 0$, soit $W_n(k)$ l'anneau des vecteurs de Witt de longueur n sur k ; si n est assez grand, on peut relever $W_n(k) \longrightarrow k$ en un homomorphisme $W_n(k) \longrightarrow M$ qui fait de M un $W_n(k)$-module de type fini. En tant que module, M est isomorphe à une somme directe de modules $W_{n_i}(k)$, $n_i \leq n$; comme chacun des $W_{n_i}(k)$ a une structure naturelle de variété algébrique sur k, on peut transporter cette structure à M, et la structure ainsi obtenue ne dépend pas du choix de l'isomorphisme $M \longrightarrow \prod W_{n_i}(k)$ choisi.

Dans tous les cas, on a donc une structure de variété algébrique sur M, d'ailleurs isomorphe à celle de l'espace affine de dimension égale à la longueur de M.

L'addition et la multiplication sont des morphismes pour cette structure ; les unités de M forment un ouvert U_M de M, et la structure induite sur U_M fait de U_M un groupe algébrique. Ce groupe est produit du groupe multiplicatif G_m (les "représentants multiplicatifs") par le groupe $U_M^{(1)}$ des éléments congrus à 1, groupe qui est unipotent.

Si N est quotient de M, le groupe U_N est quotient du groupe U_M.

Soit maintenant K un corps complet pour une valuation discrète v, soit A l'anneau de la valuation, et soit $\mathfrak{m}$ son idéal maximal. Soit $U = A - \mathfrak{m}$ le groupe des unités de A, et soit $U^{(n)} = 1 + \mathfrak{m}^n$. L'anneau $A/\mathfrak{m}^n$ est un anneau d'Artin, dont le groupe des unités s'identifie au quotient $U/U^{(n)}$; en appliquant ce qui précède, on obtient donc une structure de groupe algébrique sur $U/U^{(n)}$, et U est limite projective des groupes $U/U^{(n)}$. Le quotient $U/U^{(1)}$ n'est autre que le groupe multiplicatif G_m. Pour $n \geqslant 1$, le quotient $U^{(n)}/U^{(n+1)}$ s'identifie au groupe additif G_a ; de façon précise, soit π une uniformisante, et faisons correspondre à tout $a \in A$ la classe de $1 + a\pi^n$ dans $U^{(n)}/U^{(n+1)}$; par passage au quotient on obtient un morphisme bijectif

$$\theta_n : G_a \longrightarrow U^{(n)}/U^{(n+1)} ,$$

qui n'est pas un isomorphisme en général : c'est une isogénie radicielle de degré p^i, avec $i = [\frac{n}{e}]$, $e = v(p)$ étant l'indice de ramification absolu de K.

2. Groupes quasi-algébriques et groupes proalgébriques.

Les groupes algébriques commutatifs forment une catégorie additive qui n'est pas abélienne (sauf en caractéristique zéro), et où les produits infinis n'existent pas. On va remédier successivement à ces deux défauts :

a. Groupes quasi-algébriques. Soit G un groupe ; nous dirons que deux structures de groupes algébriques T_1, T_2 sur G sont équivalentes s'il existe une structure T_3 telle que $G_{T_1} \longrightarrow G_{T_3}$ et $G_{T_2} \longrightarrow G_{T_3}$ soient des morphismes. Un groupe G, muni d'une classe de structures de groupe algébrique pour la relation d'équivalence ci-dessus, est un groupe quasi-algébrique. Si G et G' sont deux tels groupes, un morphisme $f : G \longrightarrow G'$ est un homomorphisme dont le graphe est fermé dans $G \times G'$. On a ainsi défini une catégorie qui est abélienne (lorsqu'on se borne aux groupes commutatifs).

b. Groupes proalgébriques. Pour simplifier, on se borne au cas des groupes commutatifs. Un groupe proalgébrique G est un groupe muni d'une famille S de sous-groupes, et pour tout $H \in S$, d'une structure de groupe quasi-algébrique sur G/H. On suppose vérifiées les trois conditions suivantes :

i. $H \in S$ et $H' \in S$ entraînent $H \cap H' \in S$; les applications $G/(H \cap H') \longrightarrow G/H$ et $G/(H \cap H') \longrightarrow G/H'$ sont des morphismes.

ii. Si $H \in S$ et si $G' \supset H$, on a $G' \in S$ si et seulement si G' est image réciproque d'un sous-groupe fermé de G/H.

iii. L'application canonique de G dans la limite projective des groupes G/H est bijective.

Si G et G' sont deux tels groupes, un morphisme $f : G \longrightarrow G'$ est un homomorphisme tel que $H' \in S'$ entraîne $f^{-1}(H') \in S$, et que l'application $G/f^{-1}(H') \longrightarrow G'/H'$ soit un morphisme de groupes quasi-algébriques.

On obtient ainsi une catégorie abélienne, où l'on peut définir produits et limites projectives ; de plus, le foncteur limite projective est un foncteur exact ; l'axiome AB-5* de GROTHENDIECK [2] est vérifié. Cette catégorie a d'autres propriétés agréables ; par exemple, elle possède un cogénérateur et suffisamment d'objets projectifs.

3. Le groupe fondamental d'un groupe proalgébrique.

Soit G un groupe proalgébrique ; nous dirons que G est connexe (resp. que G est de dimension zéro) si G/H est connexe (resp. fini) pour tout $H \in S$. Tout groupe proalgébrique G contient un plus grand sous-groupe connexe G_o ; le quotient $\pi_o(G) = G/G_o$ est de dimension zéro. (Noter qu'un groupe proalgébrique de dimension zéro s'identifie à un groupe abélien compact totalement discontinu).

Un groupe proalgébrique connexe G est dit simplement connexe s'il ne possède aucune "isogénie" non triviale, c'est-à-dire si une suite exacte

$$0 \longrightarrow N \longrightarrow G' \longrightarrow G \longrightarrow 0 \text{ , avec } G' \text{ connexe, } \dim(N) = 0 \text{ ,}$$

entraîne $N = 0$.

Pour tout groupe proalgébrique G il existe un groupe simplement connexe $\bar{G}$, et un homomorphisme

$$f : \bar{G} \longrightarrow G$$

tels que Ker(f) et Coker(f) soient de dimension zéro, ce qui entraîne d'ailleurs $\mathrm{Coker}(f) = \pi_0(G)$. Le couple $(\bar{G}, f)$ est unique, à un isomorphisme unique près ; on pose :

$$\mathrm{Ker}(f) = \pi_1(G) .$$

Les groupes $\bar{G}$, $\pi_0(G)$, $\pi_1(G)$ sont des foncteurs en G . On voit tout de suite que $\bar{G}$ et $\pi_0(G)$ sont exacts à droite ; en fait :

THÉORÈME 1. - Le foncteur $\bar{G}$ est exact.

[Il revient au même de dire que le foncteur $\pi_1(G)$ est exact à gauche, ou encore, que si $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ est une suite exacte de groupes proalgébriques, elle donne naissance à une suite exacte :

$$0 \longrightarrow \pi_1(G') \longrightarrow \pi_1(G) \longrightarrow \pi_1(G'') \longrightarrow \pi_0(G') \longrightarrow \pi_0(G) \longrightarrow \pi_0(G'') \longrightarrow 0 .$$

On aurait pû également définir les $\pi_i(G)$, $i \geqslant 0$, comme les satellites gauches du foncteur $\pi_0(G)$, et le théorème 1 signifie que $\pi_i(G) = 0$ pour $i \geqslant 2$].

La démonstration est compliquée. On se ramène à montrer que, si G' est un sous-groupe connexe d'un groupe connexe G , l'homomorphisme $\pi_1(G') \longrightarrow \pi_1(G)$ est injectif. Si N est un groupe fini quelconque, on vérifie que

$$\mathrm{Hom}(\pi_1(G) , N) = \mathrm{Ext}(G , N) ,$$

avec les notations de [6] , Chapitre VII ; en utilisant alors certaines propriétés des Ext (notamment le dernier théorème de [6]) , la structure des groupes unipotents ([6] , Chapitre VII , paragraphe 2) , et le calcul des $\mathrm{Ext}(W_n , N)$, on arrive au résultat ...

4. Enoncé du théorème.

Nous reprenons les hypothèses et les notations de n° 1 : K , v , k , ... , à cela près que nous notons U_K le groupe des unités de K ; nous munissons U_K de la structure de groupe proalgébrique limite projective des structures de groupes algébriques des quotients $U_K/U_K^{(n)}$.

Soit L/K une extension galoisienne finie, de groupe de Galois g ; on sait que $\hat{H}^q(g , L^*) = 0$ pour tout $q \in \underset{\sim}{Z}$. La suite exacte :

$$(*) \qquad 0 \longrightarrow U_L \longrightarrow L^* \longrightarrow \underset{\sim}{Z} \longrightarrow 0$$

montre alors que $\hat{H}^q(g , U_L)$ s'identifie à $H^{q-1}(g , \underset{\sim}{Z})$. Pour $q = 0$, cela signifie que tout élément de U_K est norme d'un élément de U_L , ce qui est facile à vérifier directement (cf. par exemple [3]) . Si I désigne le noyau de la norme N , on a donc une suite exacte :

$$(**) \qquad 0 \longrightarrow I \longrightarrow U_L \xrightarrow{N} U_K \longrightarrow 0 .$$

De plus, N est un morphisme du groupe proalgébrique U_L dans le groupe proalgébrique U_K . Soit I_o le sous-groupe de I engendré par les $s(u)/u$, $s \in g$, $u \in U_L$; on a :

$$(***) \qquad I/I_o = \hat{H}^{-1}(g , U_L) = \hat{H}^{-2}(g , \underset{\sim}{Z}) = g/g' ,$$

en désignant par g' le groupe des commutateurs de g . En particulier, I/I_o est un groupe fini, et comme I_o est connexe (car image d'un groupe connexe), on en conclut que I_o est la composante connexe de I et que $\pi_o(I) = I/I_o$ s'identifie à g/g' .

La suite exacte d'homotopie attachée à la suite exacte (**) donne alors un homomorphisme surjectif $\pi_1(U_K) \longrightarrow g/g'$.

Prenant g abélien, et passant à la limite sur L , on obtient finalement un homomorphisme surjectif

$$\theta : \pi_1(U_K) \longrightarrow A(K) ,$$

où A(K) désigne le groupe de Galois de l'extension abélienne maximale de K .

THÉORÈME 2. - L'homomorphisme $\theta : \pi_1(U_K) \longrightarrow A(K)$ est un isomorphisme.

En d'autres termes, on vient de voir que toute extension abélienne fournit une isogénie $0 \longrightarrow g \longrightarrow U_L/I_o \longrightarrow U_K \longrightarrow 0$, et le théorème 2 affirme que l'on obtient ainsi toutes les isogénies (connexes) de U_K . Le théorème 2 est donc essentiellement un théorème d'existence ; nous donnerons au n° 6 des indications sur sa démonstration.

5. Relations avec la ramification supérieure.

Soit L/K une extension galoisienne de groupe de Galois g , et soit π une uniformisante de K . Si $x \geqslant 0$, soit g_x le sous-groupe de g formé des $s \in g$ tels que $v(1 - s(\pi)/\pi) \geqslant x$; les g_x sont les groupes de ramification de g . Si h est un sous-groupe de g , on a $h_x = g_x \cap h$.

A partir des g_x , on définit une fonction $y = \varphi(x)$, définie pour $x \geqslant 0$, continue, linéaire par morceaux, et telle que :

i. $\varphi(0) = 0$.

ii. $\varphi'_g(x) = (g : g_x)^{-1}$ (la notation φ'_g désignant la dérivée à gauche).

La fonction inverse $x = \psi(y)$ est encore linéaire par morceaux ; il est clair que $x \in \underset{\sim}{N}$ entraîne $y \in \underset{\sim}{N}$. On peut renuméroter les g_x en définissant $g^y = g_x$ chaque fois que $y = \varphi(x)$. Si h est un quotient de g , h^y est image de g^y (théorème de Herbrand, cf. [3], [4]) .

La fonction ψ est reliée à l'application norme : $U_L \longrightarrow U_K$ par le théorème suivant, dû à Hasse [3] (au langage près) :

THÉORÈME 3. - Pour tout entier $n \geqslant 1$, on a $NU_L^{\psi(n)} \subset U_K^{(n)}$ et $NU_L^{\psi(n)+1} \subset U_K^{(n+1)}$; l'application

$$N : U_L^{\psi(n)} / U_L^{\psi(n)+1} \longrightarrow U_K^{(n)} / U_K^{(n+1)}$$

est une isogénie dont le noyau s'identifie à $g_{\psi(n)}/g_{\psi(n)+1}$; le facteur séparable du degré de cette isogénie est égal à $\psi'_{d/g}(n) = \psi'_d(n)/\psi'_g(n)$.

Le théorème précédent donne des renseignements sur les isogénies "partielles" au-dessus des quotients $U_K^{(n)}/U_K^{(n+1)}$; on en déduit notamment que le degré (séparable) de l'isogénie $U_L/I_o \longrightarrow U_K$ divise le produit $\prod \psi'_{d/g}(n)$, n entier. Mais on a vu au n° 4 que, lorsque g est abélien, ce degré est égal à l'ordre de g , c'est-à-dire au produit $\prod \psi'_{d/g}(y)$, y réel $\geqslant 0$. On en conclut :

THÉORÈME 4. - Lorsque L/K est une extension abélienne, on a $\psi'_{d/g}(y) = 1$ si y n'est pas entier.

Autrement dit, si r est un entier tel que $g_r \neq g_{r+1}$, le nombre réel $n = \psi(r)$ est un entier.

On obtient tout aussi facilement :

THÉORÈME 5. - Si l'on filtre le groupe $\mathfrak{N}_1(U_K)$ par ses sous-groupes $\mathfrak{N}_1(U^{(n)})$, et le groupe de Galois $A(K) = \varprojlim g$ par ses sous-groupes $A(K)^n = \varprojlim g^n$, l'isomorphisme $\theta : \mathfrak{N}_1(U_K) \longrightarrow A(K)$ transforme la première filtration en la seconde.

[Dans la terminologie classique, le théorème 5 est la détermination du conducteur à partir de la ramification supérieure ; le théorème 4 exprime que le conducteur d'Artin est entier (dans le cas abélien, mais on passe de là au cas général par le théorème de Brauer)].

6. Démonstration du théorème 2.

Elle est analogue à la démonstration donnée par WHAPLES [7] pour le théorème d'existence du corps de classes local.

Il suffira de montrer que, pour tout groupe fini N, l'homomorphisme

$$\theta^* : \mathrm{Hom}(A(K) , N) \longrightarrow \mathrm{Hom}(\mathfrak{T}_1(U) , N)$$

est surjectif. Par dévissage, on se ramène au cas où N est cyclique d'ordre premier ℓ ; si ℓ n'est pas égal à la caractéristique de k, c'est facile (extensions "tamely ramified"). On va donc supposer que k est de caractéristique p, et que $N = \underset{\sim}{Z}/p\underset{\sim}{Z}$. Pour abréger, on écrit $H(U)$ au lieu de $\mathrm{Hom}(\mathfrak{T}_1(U) , N)$.

Notons d'abord que $H(U_K)$ est réunion des sous-groupes croissants $H(U_K/U_K^{(n)})$; on va montrer par récurrence sur n que $H(U_K/U_K^{(n)})$ est contenu dans l'image de θ^*, le cas $n = 1$ étant trivial. Pour passer de n à $n+1$, on utilise la suite exacte :

$$(1) \qquad 0 \longrightarrow H(U_K/U_K^{(n)}) \longrightarrow H(U_K/U_K^{(n+1)}) \longrightarrow H(U_K^{(n)}/U_K^{(n+1)}) .$$

Posons, comme au n° 2, $e = v(p)$, et soit $k = \frac{p}{p-1}.e$. Distinguons quatre cas :

i. $n < k$ et $(p , n) = 1$.

Soit $a \in U_K$; l'équation $x^p - x = a.\pi^{-n}$ est irréductible sur K, et définit une extension abélienne L/K dont le groupe de Galois s'identifie à $N = \underset{\sim}{Z}/p\underset{\sim}{Z}$ (cf. WHAPLES, [7], proposition 17) ; elle définit donc un élément $x_a \in \mathrm{Im}(\theta^*)$. Un calcul explicite montre que $x_a \in H(U_K^{(n+1)})$ et permet de déterminer l'image de x_a dans $H(U_K^{(n)}/U_K^{(n+1)}) = H(G_a)$; comme le groupe $H(G_a)$ est facile à expliciter, on peut vérifier que tout élément non nul de $H(G_a)$ est obtenu ainsi, et il en résulte bien que $\mathrm{Im}(\theta^*)$ contient $H(U_K^{(n+1)})$.

ii. $n < k$ et p divise n.

Posons $n = pm$; on vérifie par calcul direct que $a \longrightarrow a^p$ définit par

passage au quotient un homomorphisme surjectif

$$\lambda : U_K^{(m)}/U_K^{(n+1)} \longrightarrow U_K^{(n)}/U_K^{(n+1)}$$

dont le noyau est connexe. Considérons alors le diagramme commutatif :

$$\begin{array}{ccc} H(U_K/U_K^{(n+1)}) & \xrightarrow{\rho} & H(U_K^{(n)}/U_K^{(n+1)}) \\ \downarrow \mu^* & & \downarrow \lambda^* \\ H(U_K/U_K^{(n+1)}) & \xrightarrow{\sigma} & H(U_K^{(m)}/U_K^{(n+1)}) \end{array},$$

où ρ et σ sont les homomorphismes transposés des inclusions, et où μ^* est le transposé de $a \longrightarrow a^p$. Il est clair que $\mu^* = 0$. Comme le noyau de λ est connexe, λ^* est injectif, et il en résulte que

$$\rho = 0 , \quad \text{et} \quad H(U_K^{(n+1)}) = H(U_K^{(n)}) .$$

iii. $n > k$.

On raisonne comme dans (ii) , en posant $m = n - e$.

(iv) $n = k$ (ceci n'est possible que si K contient une racine p-ème de l'unité).

On montre, par un raisonnement analogue à ceux de (ii) et (iii) que l'image de $H(U_K/U_K^{(n+1)})$ dans $H(U_K^{(n)}/U_K^{(n+1)}$ a au plus p éléments. D'autre part, l'équation $x^p - \pi = 0$ fournit un élément de $\mathrm{Im}(\theta^*)$, dont on vérifie qu'il est dans $H(U_K/U_K^{(n+1)})$ et que son image dans $H(U_K^{(n)}/U_K^{(n+1)})$ n'est pas nulle. D'où le résultat cherché.

REMARQUE. - Dans le cas d'égale caractéristique, on peut donner une démonstration beaucoup plus directe du théorème 2 , analogue à celle de la théorie de Lang.

7. Raccord avec le corps de classes local.

On suppose maintenant que le corps des restes k de K est un corps fini à q éléments ; soit F la clôture algébrique de k . Soit $\hat{K}_{nr}$ le complété de l'extension non ramifiée maximale de K , et soit $U_{nr}(K)$ son groupe des unités. Le corps des restes de $\hat{K}_{nr}$ est F , on peut donc appliquer les résultats du numéro précédent à ce corps. En outre, une construction analogue à celle du numéro 1 permet de munir les groupes $U_{nr}(K)/U_{nr}(K)^{(n)}$ d'une structure

de k-groupe algébrique, dont les points rationnels sur k ne sont autres que les éléments de $U_K/U_K^{(n)}$.

Si L/K est une extension abélienne totalement ramifiée, l'isogénie déduite de $N : U_{nr}(L) \longrightarrow U_{nr}(K)$ est définie sur k , et abélienne sur k . Or , lorsque l'on a une isogénie $f : G' \longrightarrow G$ définie sur k , et de noyau g formé de points rationnels sur k , on peut définir (LANG) un isomorphisme $G_k/G'_k \longrightarrow g$ au moyen de la substitution de Frobenius : si $x \in G_k$, on lui fait correspondre l'élément $s \in g$ tel que $f(x') = x$ entraîne $x'^q - x' = s$. On obtient donc ici un isomorphisme $f : U_K/NU_L \longrightarrow g$; on le prolonge en un isomorphisme de K^*/NL^* sur g en posant $f(\pi) = 0$ si π est une uniformisante de K qui est norme dans L .

L'isomorphisme $f : K^*/NL^* \longrightarrow g$ que nous venons de définir coïncide au signe près (cf. DWORK [1] , théorème 1) avec celui de la théorie du corps de classes local ; sa définition met en évidence ses propriétés de façon très commode.

[Tout ceci s'applique aussi lorsqu'on suppose seulement que k est un corps quasi-fini] .

BIBLIOGRAPHIE

[1] DWORK (Bernard). - Norm residue symbol in local number fields, Abh. Math. Sem. Univ. Hamburg, t. 22, 1958, p. 180-190.

[2] GROTHENDIECK (Alexander). - Sur quelques points d'algèbre homologique, Tôhoku math. J., Série 2, t. 9, 1957, p. 119-221.

[3] HASSE (Helmut). - Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper, J. Fac. Sc. Tokyo, Section 1, t. 2, 1929-1934, p. 477-498.

[4] HERBRAND (Jacques). - Théorie arithmétique des corps de nombres de degré infini, II : Extensions algébriques de degré infini, Math. Annalen, t. 108, 1933, p. 699-717.

[5] LANG (Serge). - Sur les séries L d'une variété algébrique, Bull. Soc. math. France, t. 84, 1956, p. 385-407.

[6] SERRE (Jean-Pierre). - Groupes algébriques et corps de classes. - Paris, Hermann, 1959. (Act. scient. et ind., 1264, Publ. Inst. Uni. Nancago, 7).

[7] WHAPLES (G.). - Generalized local class field theory, II : Existence theorem, Duke math. J., t. 21, 1954, p. 247-255.