SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Cohomologie galoisienne : progrès et problèmes

Séminaire N. Bourbaki, 1993-1994, exp. n° 783, p. 229-257.

<http://www.numdam.org/item?id=SB_1993-1994__36__229_0>

Séminaire BOURBAKI
46ème année, 1993-94, n° 783

Mars 1994

COHOMOLOGIE GALOISIENNE : PROGRÈS ET PROBLÈMES

par **Jean-Pierre SERRE**

NOTATIONS

Le corps de base est noté F. On en choisit une clôture séparable F_s et l'on note Γ_F le groupe de Galois $\mathrm{Gal}(F_s/F)$.

Sauf mention expresse du contraire, tous les groupes algébriques considérés sont *définis sur* F, *lisses* et *linéaires* : on ne parlera pas des variétés abéliennes.

PRÉLIMINAIRES

§ 1. RAPPELS SUR $H^1(F, G)$

Soit G un groupe algébrique sur F. On s'intéresse à l'ensemble $H^1(F, G)$, ensemble que l'on peut définir de deux façons équivalentes ([32], Chap. III, § 1) :

- classes d'isomorphisme de G-torseurs (G-torseur = espace homogène principal à droite de G)

- classes d'équivalence de 1-cocycles $z : \Gamma_F \to G(F_s)$, cf. [32], Chap. I, § 5.

(Rappelons comment on passe du point de vue "torseur" au point de vue "cocycle". Si P est un G-torseur, P est lisse (puisque G l'est), donc possède un point rationnel sur F_s. Soit $x \in P(F_s)$ un tel point. Si $\gamma \in \Gamma_F$, on a $\gamma(x) \in P(F_s)$. Il existe donc un unique élément $z(\gamma)$ de $G(F_s)$ tel que $\gamma(x) = x.z(\gamma)$. L'application $z : \Gamma_F \to G(F_s)$ ainsi définie est un 1-cocycle dont la classe d'équivalence ne dépend pas du choix de x.)

Ainsi, déterminer $H^1(F, G)$ revient à *classer les G-fibrés principaux sur une base réduite à un seul point*, à savoir le point $\mathrm{Spec}(F)$. Comme on sait, ce problème est moins facile qu'il n'en a l'air à première vue ; la topologie (étale) de Spec(F) est loin d'être triviale !

Pourquoi s'intéresser à $H^1(F,G)$? La principale raison est que $H^1(F,G)$ *classifie les F-formes de tout "objet algébrique" A dont G est le groupe des automorphismes.* (Par "objet algébrique", j'entends une variété algébrique munie de données supplémentaires, par exemple un groupe algébrique, ou un espace vectoriel muni de tenseurs.) Rappelons (cf. [32], *loc. cit.*) que, si A' est une F-forme de A, on lui associe le G-torseur $P = \mathrm{Isom}(A, A')$; en sens inverse, si $z : \Gamma_F \to G(F_s)$ est un 1-cocycle, on lui associe l'objet $A' = {}_zA$ déduit de A par *torsion* au moyen de z.

(Attention : pour que ceci soit correct, on doit supposer que G est le foncteur des automorphismes de l'objet A ; en particulier, ce foncteur doit être lisse.)

Exemples

(1) Prenons pour A, soit l'algèbre des matrices $\mathbf{M}_n$ munie de sa structure d'algèbre, soit l'espace projectif $\mathbf{P}_{n-1}$ muni de sa structure de variété projective. Dans les deux cas, on a $\mathrm{Aut}(A) = \mathbf{PGL}_n$ (quotient du groupe $\mathbf{GL}_n$ par son centre $\mathbf{G}_m$). Or les F-formes de $\mathbf{M}_n$ sont les algèbres centrales simples sur F de rang n^2, et les F-formes de $\mathbf{P}_{n-1}$ sont les variétés de Severi-Brauer de dimension $n-1$. D'où des bijections entre les trois ensembles suivants :

- $H^1(F, \mathbf{PGL}_n)$;
- classes d'isomorphisme des algèbres centrales simples sur F de rang n^2 ;
- classes d'isomorphisme des variétés de Severi-Brauer de dimension $n-1$.

Pour $n = 2$, cela redonne la correspondance bien connue entre algèbres de quaternions et courbes de genre 0.

(2) Prenons pour A l'objet (V, q) formé d'un F-espace vectoriel V de dimension n et d'une forme quadratique non dégénérée q sur V. Le foncteur des automorphismes de A est le groupe orthogonal $\mathbf{O}(q)$ de q. Si la caractéristique de F est $\neq 2$ (ou si n est pair), $\mathbf{O}(q)$ est lisse. D'où des bijections entre :

- $\mathbf{H}^1(F, \mathbf{O}(q))$;
- classes de formes quadratiques non dégénérées de rang n sur F.

(3) Pour d'autres exemples, relatifs aux groupes exceptionnels G_2 et F_4, voir §§ 8, 9.

Tout ceci, qui est bien connu depuis la fin des années 50, explique que la structure de $H^1(F,G)$ ait été beaucoup étudiée, le cas le plus intéressant étant celui où G est réductif (et même semi-simple). Comme on le verra, les résultats dépendent de façon essentielle de la dimension cohomologique du groupe profini Γ_F.

§ 2. LES NOMBRES PREMIERS ASSOCIÉS À UN TYPE DE GROUPE SIMPLE

2.1. Absence de structure de groupe sur $H^1(F,G)$

Lorsque G est commutatif, $H^1(F,G)$ est un groupe (commutatif), et l'on peut définir les groupes $H^i(F,G)$ pour tout $i \geq 0$. Dans le cas général, la structure de groupe est remplacée par :

– un élément distingué (noté 0 ou 1), qui correspond au torseur trivial $P = G$ et fait de $H^1(F,G)$ un *ensemble pointé* ; cela permet de parler de *noyaux* et de *suites exactes*, cf. [32], Chap. I, § 5 ;

– une opération de *translation* : si z est un 1-cocycle : $\Gamma_F \to G(F_s)$, et si ${}_zG$ désigne le groupe déduit de G par torsion au moyen de z (vis-à-vis de l'action de G sur G par automorphismes intérieurs), on a une bijection :

$$\tau_z : H^1(F, {}_zG) \longrightarrow H^1(F,G)$$

qui transforme 0 en la classe de z ([32], Chap. I, n° 5.3).

2.2. L'ensemble $S(G)$

Bien que $H^1(F,G)$ ne soit pas un groupe, certains nombres premiers jouent un rôle spécial dans sa structure. Je vais me borner à définir l'ensemble de ces nombres premiers, noté $S(G)$, dans le cas particulier le plus important, celui où G est semi-simple connexe et où son système de racines R (sur F_s) est irréductible ; un tel groupe est dit *absolument presque simple.* L'ensemble $S(G)$ est alors formé des nombres premiers p satisfaisant à l'une des conditions suivantes :

2.2.1. p divise l'ordre du groupe d'automorphismes du graphe de Dynkin de G.

2.2.2. p divise l'indice du réseau des racines dans le réseau des poids (autrement dit l'ordre du centre du revêtement universel $\widetilde{G}$ de G).

2.2.3. p est un nombre premier *de torsion* pour R, au sens usuel de ce terme dans la topologie des groupes de Lie (cf. [7], p. 775-776).

(Une autre façon d'énoncer 2.2.1 et 2.2.2 est de dire que p divise l'ordre du groupe d'automorphismes du *graphe de Dynkin complété* de R, cf. Bourbaki, LIE VI, § 4, n° 3.)

Le tableau suivant donne $S(G)$ pour les différents types de systèmes de racines :

Type	**Éléments de** $S(G)$
A_n	2, et les diviseurs premiers de $n+1$
B_n, C_n, D_n $(n \neq 4)$, G_2	2
D_4, F_4, E_6, E_7	2 et 3
E_8	2, 3 et 5

2.3. Un théorème de Tits

Pour énoncer le résultat, convenons de dire que, si S est un ensemble de nombres premiers, un entier est *S-primaire* si tous ses facteurs premiers appartiennent à S.

Théorème 1 – *Supposons G absolument presque simple* (cf. ci-dessus). *Pour tout* $x \in H^1(F,G)$*, il existe une extension finie* F_x *de* F *ayant les deux propriétés suivantes :*

(a) *Le degré* $[F_x : F]$ *de* F_x *sur* F *est* $S(G)$*-primaire.*

(b) F_x *"tue"* x*, autrement dit l'image de* x *dans* $H^1(F_x, G)$ *est* 0.

(Si P est un G-torseur correspondant à x, la condition (b) signifie que P a un point rationnel sur K_x.)

Ce résultat est essentiellement dû à Tits (voir [40]). De façon plus précise, Tits définit un certain entier $S(G)$-primaire N et démontre :

(c) Il existe une extension finie F' de F, de degré divisant N, telle que G devienne déployé sur F'.

En appliquant ce résultat au groupe tordu ${}_zG$ (où z est un 1-cocycle représentant x), avec comme corps de base le corps F', on obtient une extension F'' de F', de degré divisant N, sur laquelle ${}_zG$ devient déployé. Il n'est pas difficile de voir que cela entraîne que F'' tue x. On peut donc prendre $F_x = F''$, ce qui démontre le théorème (sous une forme plus précise, puisque le degré de F'' sur F divise N^2).

Remarques

(1) On peut sans doute exiger que F_x soit une extension *séparable* de F, mais je ne l'ai pas vérifié.

(2) Un énoncé un peu plus faible que le th. 1 avait été démontré par Grothendieck ([12]) en 1958.

(3) Dans l'énoncé du th. 1, on ne peut pas remplacer $S(G)$ par un ensemble strictement plus petit, ne dépendant que du système de racines de G.

2.4. Quelques questions

Conservons les notations ci-dessus. Disons qu'un entier est *premier à* $S(G)$ si aucun de ses facteurs premiers n'appartient à $S(G)$.

Question 1 – *Est-il vrai que, si une extension finie F'/F a un degré premier à $S(G)$, l'application $H^1(F,G) \to H^1(F',G)$ est injective ?*

Cela paraît très optimiste, mais je ne connais pas de contre-exemple. C'est en tout cas vrai (avec $S(G) = \{2\}$) pour les groupes orthogonaux (Springer [34]), les groupes unitaires (Bayer-Lenstra [4]), et le groupe G_2 (voir § 8). C'est également vrai chaque fois que l'on peut décrire $H^1(F,G)$ au moyen d'*invariants cohomologiques* (voir §§ 6, 7), car ceux-ci ne font intervenir que des groupes de coefficients qui sont $S(G)$-primaires.

Voici une question encore plus optimiste :

Question 2 – *Soient F_i/F des extensions finies telles que le* pgcd *des $[F_i : F]$ soit premier à $S(G)$. Est-il vrai que l'application*

$$H^1(F,G) \longrightarrow \prod_i H^1(F_i,G)$$

est injective ?

Noter que l'hypothèse sur les $[F_i : F]$ est satisfaite si ces entiers sont premiers entre eux. Même le cas de deux extensions F' et F'' avec $[F' : F] = 2$, $[F'' : F] = 3$ n'est pas connu.

CORPS DE DIMENSION 1 OU 2

§ 3. RÉSULTATS AUXILIAIRES SUR LES TORES MAXIMAUX

Rappelons qu'un groupe semi-simple est dit *quasi-déployé* s'il possède un sous-groupe de Borel (défini sur le corps de base, bien entendu).

Théorème 2 – *Supposons G semi-simple connexe quasi-déployé. Pour tout $x \in H^1(F,G)$ il existe un tore maximal T de G tel que x appartienne à l'image de $H^1(F,T) \to H^1(F,G)$.*

Lorsque F est parfait, ce résultat est dû à Steinberg ([37], th. 11.1). D'après Borel et Springer ([8], n° 8.6), les arguments de Steinberg peuvent être étendus au cas général.

Voici un résultat sur les $H^1(F,T)$, dû à Harder ([13], I, § 3) et Tits ([39], prop. 4) :

Théorème 3 – *Supposons G absolument presque simple* (cf. n° 2.2). *Soit $S = \{2,3\}$ si G est de type G_2 et $S = S(G)$ sinon. Si T est un tore maximal de G, le groupe $H^1(F,T)$ est un groupe de torsion S-primaire* (i.e. la p-composante de $H^1(F,T)$ est 0 si $p \notin S$).

(*Exemple* : si G est de type E_8, $H^1(F,T)$ ne contient pas d'élément d'ordre 7.)

Ce théorème se démontre sans difficulté, à partir du lemme suivant, qui se vérifie cas par cas :

Lemme 1 – *Soient R le système de racines de G et P le réseau des poids de R. Soit Γ un p-groupe d'automorphismes de R, avec $p \notin S$. Il existe alors un sous-réseau P' de P, d'indice premier à p, qui possède une $\mathbf{Z}$-base stable par Γ.*

§ 4. LE CAS DE DIMENSION 1

4.1. Dimension cohomologique (cf. [32], Chap. I, § 3)

Soient Γ un groupe profini et p un nombre premier. On appelle *p-dimension* *cohomologique* de Γ, et on note $\mathrm{cd}_p(\Gamma)$ la borne supérieure des entiers i tels qu'il existe un Γ-module fini p-primaire C avec $H^i(\Gamma, C) \neq 0$.

On a $\mathrm{cd}_p(\Gamma) \leq 1$ (resp. $\mathrm{cd}_p(\Gamma) = 0$) si et seulement si les p-sous-groupes de Sylow de Γ sont des pro-p-groupes libres (resp. sont triviaux).

Ceci s'applique notamment au groupe $\Gamma_F = \mathrm{Gal}(F_s/F)$.

4.2. Le théorème de Steinberg (ex-"conjecture I", cf. [31], [32])

Théorème 4 ([37], th. 11.12) – *Supposons que F soit parfait et que $\mathrm{cd}_p(\Gamma_F) \leq 1$ pour tout nombre premier p. Soit G un groupe linéaire connexe sur F. On a* $H^1(F, G) = 0$. (Autrement dit, tout G-torseur est trivial.)

L'hypothèse que F est parfait permet de se débarrasser du radical unipotent et l'on peut supposer que G est, soit un tore, soit un groupe semi-simple. Le cas d'un tore est facile. Si G est semi-simple, on remarque que G est isomorphe à un "tordu" ${}_zG_0$, où G_0 est quasi-déployé, et z est un 1-cocycle à valeurs dans le groupe adjoint G_0^{adj} de G_0. Or le th. 2 entraîne que $H^1(F, G_0^{\mathrm{adj}}) = 0$. On a donc $G \approx G_0$, d'où $H^1(F, G) = 0$ en appliquant à nouveau le th. 2.

On a démontré en même temps :

Corollaire 1 – *Tout groupe semi-simple sur F est quasi-déployé.*

Mentionnons aussi le résultat suivant, dû à Springer (cf. [32], Chap. III, n° 2.4), qui est à la fois un corollaire et une généralisation du th. 4 :

Corollaire 2 – *Tout espace homogène de G a un point rationnel.*

Voici quelques *exemples* de corps satisfaisant aux hypothèses du th. 4 : corps finis (où l'on retrouve un théorème de Lang [20], d'ailleurs applicable aux groupes algébriques connexes non nécessairement linéaires) ; corps locaux de caractéristique 0 à corps résiduel algébriquement clos ; extensions algébriques de $\mathbf{Q}$ contenant toutes les racines de l'unité ; extensions de degré de transcendance 1 d'un corps algébriquement clos de caractéristique 0 (e.g. corps des fonctions méromorphes sur une surface de Riemann compacte).

4.3. Extension du théorème de Steinberg au cas d'un corps imparfait

Soit p la caractéristique de F, supposée $\neq 0$. La condition $\mathrm{cd}_p(\Gamma_F) \leq 1$ est satisfaite quel que soit F, cf. [32], Chap. II, n° 2.2. Il y a lieu de la renforcer en demandant :

(1_p) – *Pour toute extension finie séparable F' de F, la p-composante du groupe de Brauer de F' est* 0 (avec les notations du § 10, cela signifie que $H^2_p(F') = 0$).

Un corps F satisfaisant à (1_p), ainsi qu'à $\mathrm{cd}_q(\Gamma_F) \leq 1$ pour tout nombre premier q, est dit "de dimension ≤ 1" (autre caractérisation : le groupe de Brauer de toute extension finie séparable de F est 0). On a pour ces corps un analogue (un peu plus faible) du théorème de Steinberg :

Théorème 4′ ([8], n° 8.6) – *Si F est de dimension ≤ 1, et si G est un groupe réductif connexe sur F, on a $H^1(F, G) = 0$.*

Noter l'hypothèse "G est réductif" ; l'énoncé ne serait pas vrai si l'on acceptait des groupes connexes quelconques, par exemple unipotents.

Remarque – Inversement, si $H^1(F, G) = 0$ pour tout G semi-simple connexe, le corps F est de dimension ≤ 1 (facile).

4.4. Une variante

Supposons G absolument presque simple, et soit $S(G)$ l'ensemble de nombres premiers correspondant, cf. n° 2.2. L'énoncé suivant précise les th. 4 et 4′ :

Théorème 4″ – *On a $H^1(F, G) = 0$ si $\mathrm{cd}_p(\Gamma_F) \leq 1$ pour tout $p \in S(G)$, et si la condition* (1_p) *est satisfaite* (pour $p = \mathrm{caract}(F)$, bien entendu).

On utilise les hypothèses cohomologiques, combinées avec le th. 3, pour prouver que $H^1(F, T) = 0$ pour tout tore maximal T (sauf si G est de type G_2, auquel cas $H^1(F, T)$ peut contenir des éléments d'ordre 3 — mais ceux-ci ont une image nulle dans $H^1(F, G)$). L'argument de Steinberg s'applique alors sans changement.

Remarque – On peut même supprimer la condition (1_p) si la caractéristique p de F n'appartient pas à $S(G)$.

§5. LE CAS DE DIMENSION 2

On vient de voir que :

$$\mathrm{cd} \leq 1 \iff \text{nullité de } H^1(F,G) \text{ pour } G \text{ connexe.}$$

On va maintenant s'occuper de :

$$\mathrm{cd} \leq 2 \overset{?}{\iff} \text{nullité de } H^1(F,G) \text{ pour } G \text{ simplement connexe.}$$

L'hypothèse "cd ≤ 2" est satisfaite par les corps p-adiques et les corps de nombres totalement imaginaires. Commençons par ceux-là :

5.1. Corps locaux

On suppose que F est complet pour une valuation discrète ; on note k son corps résiduel.

Théorème 5 (Kneser [17]) – *Supposons k fini* (autrement dit F localement compact). *On a alors $H^1(F,G) = 0$ pour tout G semi-simple simplement connexe.*

La démonstration de Kneser procède cas par cas : $A_n, B_n, \cdots, E_8$. La théorie des immeubles de Bruhat-Tits donne une démonstration plus directe : elle permet de comparer $H^1(F,G)$ à certains $H^1(k,G_i)$, où les G_i sont des groupes linéaires connexes sur le corps résiduel k. Compte tenu du th. 4, cela entraîne :

Théorème 5′ (Bruhat-Tits [9], n° 4.7) – *L'énoncé du th. 5 reste valable lorsqu'on y remplace l'hypothèse "k est fini" par "k est parfait de dimension ≤ 1"* (au sens du n° 4.3).

Question – *Dans le th. 5′, est-il possible de remplacer l'hypothèse que k est parfait par $[k : k^p] \leq p$, où $p =$* caract(k) ?

5.2. Corps globaux

On suppose que F est un corps global, i.e. un corps de nombres algébriques, ou un corps de fonctions d'une variable sur un corps fini.

Théorème 6 – *Si F n'a pas de place réelle, on a $H^1(F,G) = 0$ pour tout G semi-simple simplement connexe.*

Lorsque F est de caractéristique $\neq 0$, ce théorème a été démontré par Harder [14].

Lorsque F est un corps de nombres, on se ramène facilement au cas où G est absolument presque simple. La nullité de $H^1(F,G)$ se démontre alors cas par cas :

– lorsque G est de type classique (Kneser [18]) ;

– lorsque G est de type D_4 trialitaire, G_2, F_4, E_6, E_7 (Harder [13]) ;

– lorsque G est de type E_8 (Chernousov [10]).

On trouvera dans [27], § 6.7 et § 6.8, un exposé détaillé de ces divers cas ; celui de E_8 est particulièrement intéressant.

Lorsque F est un corps de nombres ayant des places réelles, le th. 6 est remplacé par le suivant (cf. [27], *loc. cit.*) :

Théorème 6′ – *Soit* Σ *l'ensemble des places réelles de* F ; *pour tout* $\sigma \in \Sigma$, *soit* F_σ *le complété de* F *pour* σ (isomorphe à $\mathbf{R}$). *Si* G *est semi-simple simplement connexe, l'application canonique*

$$H^1(F,G) \longrightarrow \prod_{\sigma\in\Sigma} H^1(F_\sigma,G)$$

est bijective.

Par exemple, si G est de type F_4, ou E_8, et si le nombre des places réelles de F est r_1, l'ensemble $H^1(F,G)$ a 3^{r_1} éléments.

Remarque – Le th. 6′, combiné avec le th. 5, entraîne que le *principe de Hasse* est vrai pour un groupe semi-simple simplement connexe. Ce principe joue un rôle important dans la démonstration du fait que *le nombre de Tamagawa d'un groupe simplement connexe est égal à* 1 (Kottwitz [19]).

5.3. La conjecture II

C'est la suivante (cf. [31], ainsi que [32], Chap. III, § 3) :

Conjecture II – *Si* F *est un corps parfait tel que* $\mathrm{cd}_p(\Gamma_F) \leq 2$ *pour tout nombre premier* p, *on a* $H^1(F,G) = 0$ *pour tout* G *semi-simple simplement connexe.*

Cette conjecture entraîne les th. 5 et 6, du moins lorsque F est de caractéristique 0.

Exemples de groupes semi-simples simplement connexes pour lesquels la conjecture a été démontrée :

– Les groupes de type A_n intérieur, autrement dit les groupes **SL** associés aux algèbres centrales simples (Merkurjev-Suslin, cf. th. 7 ci-dessous) ;

– Les groupes de spineurs (Merkurjev, non publié), et en particulier tous les groupes de type B_n ;

– Les groupes de type C_n et D_n (sauf D_4 trialitaire) et les formes extérieures de type A_n (Bayer-Parimala [5]) ;

– Les groupes de type G_2 et F_4 (cf. §§ 8, 9).

Bref, il ne reste à traiter “que” les types E_6, E_7, E_8 et D_4 trialitaire.

5.4. Un théorème de Merkurjev-Suslin

Si D est une algèbre centrale simple sur F, de rang n^2, on note $\mathbf{SL}_D$ le “F-groupe algébrique des éléments de D de norme réduite 1”. C'est une F-forme (intérieure) de $\mathbf{SL}_n$; en particulier, c'est un groupe semi-simple (et même absolument presque simple si $n > 1$) simplement connexe. On a :

$$H^1(F, \mathbf{SL}_D) = F^*/\mathrm{Nrd}(D^*),$$

de sorte que la nullité de $H^1(F, \mathbf{SL}_D)$ équivaut à dire que tout élément de F est norme réduite d'un élément de D.

Théorème 7 ([38], th. 24.8) – *Supposons F parfait. Les deux propriétés suivantes sont équivalentes* :

(a) $\mathrm{cd}_p(\Gamma_F) \leq 2$ *pour tout nombre premier* p.

(b) $H^1(F', \mathbf{SL}_{D'}) = 0$ *pour toute extension finie F' de F et toute algèbre centrale simple D' sur F'.*

Noter que $H^1(F', \mathbf{SL}_{D'})$ peut être identifié à $H^1(F, R_{F'/F}(\mathbf{SL}_{D'}))$, où $R_{F'/F}$ est le foncteur de restriction des scalaires de F' à F. La propriété (b) équivaut donc à dire que $H^1(F, G) = 0$ pour tout G de la forme $R_{F'/F}(\mathbf{SL}_{D'})$. D'où l'énoncé suivant, qui est une *réciproque* de la Conjecture II :

Corollaire – *Si F est parfait, et si $H^1(F, G) = 0$ pour tout G semi-simple simplement connexe, on a $\mathrm{cd}_p(\Gamma_F) \leq 2$ pour tout p.*

5.5. Renforcements de la conjecture II

Les hypothèses faites sur F sont un peu trop restrictives. Si G est absolument presque simple, il devrait suffire que $\mathrm{cd}_p(\Gamma_F) \leq 2$ pour tout $p \in S(G)$. Quant à la condition "F est parfait", il est sans doute possible de la supprimer si la caractéristique p de F n'appartient pas à $S(G)$; si $p \in S(G)$, on devrait pouvoir la remplacer par $[F : F^p] \leq p^2$ et $H^3_p(F') = 0$ pour toute extension finie séparable F' de F, cf. § 10.

INVARIANTS COHOMOLOGIQUES

§ 6. INVARIANTS COHOMOLOGIQUES : PREMIERS EXEMPLES

L'une des façons les plus commodes d'étudier $H^1(F, G)$ consiste à définir des applications de cet ensemble dans des groupes de cohomologie plus aisément accessibles (tout comme on associe à un fibré vectoriel des classes de Chern). Cela conduit à la notion d'*invariant cohomologique*, dont nous allons maintenant nous occuper.

6.1. Définition

Soit C un Γ_F-module de torsion (par exemple $\mathbf{Z}/n\mathbf{Z}(d) = \mu_n^{\otimes d}$, où n est premier à la caractéristique, et d est un entier). Soit i un entier > 0. Comme d'habitude en cohomologie galoisienne, posons :

$$H^i(F, C) = H^i(\Gamma_F, C).$$

Soit G un groupe algébrique sur F. Un *invariant cohomologique* de type (i, C) sur les G-torseurs est un *morphisme* du foncteur $L \mapsto H^1(L, G)$ dans le foncteur $L \mapsto H^i(L, C)$, où L parcourt la catégorie des extensions (finies ou infinies) de F.

De façon un peu plus concrète, un tel invariant est une loi $a : P \mapsto a(P)$ qui attache à tout G-torseur P sur une extension L de F un élément $a(P)$ de $H^i(L, C)$, avec la condition suivante :

(*) Si L'/L est une extension, et si P' est le G-torseur sur F' déduit de P par le changement de base $L \to L'$, l'invariant $a(P')$ de P' est l'image de $a(P)$ par l'homomorphisme $H^i(L, C) \to H^i(L', C)$.

En d'autres termes, le diagramme

$$\begin{array}{ccc} H^1(L,G) & \xrightarrow{a} & H^i(L,C) \\ \downarrow & & \downarrow \\ H^1(L',G) & \xrightarrow{a} & H^i(L',C) \end{array}$$

doit être commutatif.

Remarques

1) Il s'agit ici d'invariant "primaire", pour employer le langage de la Topologie des années 40 ; il y aurait lieu de définir aussi des invariants "supérieurs", mais je ne m'y risquerai pas.

2) Il n'y a pas de raison de se borner à des invariants "cohomologiques" : on peut avoir intérêt à définir des invariants dans des groupes de Witt ou encore dans des groupes de K-théorie du genre $K_iL/n.K_iL$.

3) L'idéal est de disposer d'un invariant qui soit précis (i.e. injectif) et calculable effectivement. Cela arrive parfois, cf. n° 7.2 et § 8.

6.2. Exemple : le cobord associé au revêtement universel

Supposons G semi-simple, et soit $\widetilde{G}$ son revêtement universel. On a une suite exacte :

$$1 \longrightarrow C \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1,$$

où C est un groupe algébrique de dimension 0, de type multiplicatif, contenu dans le centre de $\widetilde{G}$. Supposons que C soit *lisse*, autrement dit que son ordre ne soit pas divisible par la caractéristique de F ; on peut alors identifier C à l'ensemble de ses F_s-points, qui est un Γ_F-module fini. Pour toute extension L de F, on a une suite exacte de cohomologie (cf. [32], Chap. I, § 5.7) :

$$H^1(L,\widetilde{G}) \longrightarrow H^1(L,G) \xrightarrow{\Delta} H^2(L,C).$$

L'application $\Delta : H^1(L,G) \to H^2(L,C)$ intervenant dans cette suite exacte est une *opération cohomologique de type* $(2,C)$. Elle est injective si l'on a (par exemple) $H^1(L,{}_z\widetilde{G}) = 0$ pour tout 1-cocycle z de Γ_L à valeurs dans G ; d'où l'intérêt de disposer de la conjecture II.

Exemples

(a) Si $G = \mathbf{PGL}_n$, on a $\widetilde{G} = \mathbf{SL}_n$, $C = \mu_n$, d'où un invariant cohomologique

$$H^1(L, \mathbf{PGL}_n) \longrightarrow H^2(L, \mu_n) = \mathrm{Br}_n(L)$$

qui est injectif.

(b) Si $G = \mathbf{SO}(q)$, où q est une forme quadratique non dégénérée de rang ≥ 3, on a $\widetilde{G} = \mathbf{Spin}(q)$ et $C = \mu_2 = \mathbf{Z}/2\mathbf{Z}$, si la caractéristique est $\neq 2$. D'où un invariant cohomologique

$$H^1(L, \mathbf{SO}(q)) \longrightarrow H^2(L, \mathbf{Z}/2\mathbf{Z}),$$

qui est étroitement lié à l'invariant de Hasse-Witt w_2 (cf. n° 6.3, ainsi que [33], n° 2.1).

Remarque – Il y a des définitions analogues si C n'est pas lisse, à condition de définir $H^2(L, C)$ en termes de cohomologie plate et non plus de cohomologie galoisienne.

6.3. Exemple : classes de Stiefel-Whitney

Supposons F de caractéristique $\neq 2$. Soit q une forme quadratique non dégénérée sur F, de rang n, et soit $\mathbf{O}(q)$ le groupe orthogonal correspondant. Soit L une extension de F. On sait (cf. § 1, exemple 2) que les éléments de $H^1(L, \mathbf{O}(q))$ correspondent aux classes de formes quadratiques non dégénérées sur L, de même rang n que q. Si $x \in H^1(L, \mathbf{O}(q))$, notons q_x la forme quadratique correspondante, qui est définie à isomorphisme près. Pour tout $i > 0$, on peut associer à q_x sa *i-ème classe de Stiefel-Whitney* $w_i(q_x)$, qui est un élément de $H^i(L, \mathbf{Z}/2\mathbf{Z})$. On obtient ainsi un invariant cohomologique

$$w_i : H^1(L, \mathbf{O}(q)) \longrightarrow H^i(L, \mathbf{Z}/2\mathbf{Z})$$

de type $(i, \mathbf{Z}/2\mathbf{Z})$. Les cas $i = 1$ et $i = 2$ ont des interprétations simples : discriminant et invariant de Hasse-Witt. Les cas $i = 3, 4, \cdots$ sont moins utiles ; par exemple w_3 est le cup-produit de w_1 et w_2 ; quant à w_4, on a souvent intérêt à le remplacer par l'invariant d'Arason (cf. n° 7.1), qui appartient à $H^3(L, \mathbf{Z}/2\mathbf{Z})$.

§ 7. INVARIANTS COHOMOLOGIQUES À VALEURS DANS H^3

Les invariants du § 6 fournissent peu de renseignements dans le cas le plus intéressant, celui où G est semi-simple simplement connexe. Nous allons voir qu'il y a des invariants à valeurs dans H^3 qui sont plus efficaces.

7.1. Le cas de Spin(q) : invariant d'Arason

Renenons à la situation du n° 6.3, où q est une forme quadratique non dégénérée de rang n sur F. Supposons caract$(F) \neq 2$, et $n \geq 3$. Prenons pour G le groupe $\mathbf{Spin}(q)$, revêtement universel de $\mathbf{SO}(q)$. Si $\widetilde{x} \in H^1(F, G)$, notons x l'image de $\widetilde{x}$ dans $H^1(F, \mathbf{O}(q))$, et soit q_x la forme quadratique déduite de q par torsion au moyen de x.

Soit WF l'anneau de Witt de F, et soit $I = \text{Ker} : WF \to \mathbf{Z}/2\mathbf{Z}$ son idéal d'augmentation. Les formes q_x et q ont même rang, et mêmes invariants w_1 et w_2, cf. n° 6.3. Il en résulte (cf. Milnor [24]) que l'élément $q_x - q$ de WF appartient à I^3. Or il existe un *homomorphisme canonique*

$$a : I^3/I^4 \longrightarrow H^3(F, \mathbf{Z}/2\mathbf{Z}),$$

construit par Arason [1], Satz 5.7. (L'existence de cet homomorphisme est un cas particulier de la *conjecture de Milnor, loc. cit.*, disant que $I^m/I^{m+1} \cong H^m(F, \mathbf{Z}/2\mathbf{Z})$ pour tout $m \geq 0$, conjecture qui est maintenant démontrée pour $m \leq 4$.) On peut donc définir un *invariant* de $\widetilde{x}$ par $\widetilde{x} \mapsto a(q_x - q) \in H^3(F, \mathbf{Z}/2\mathbf{Z})$. En remplaçant F par une extension L quelconque, on obtient ainsi un *invariant cohomologique*

$$a : H^1(L, \mathbf{Spin}(q)) \longrightarrow H^3(L, \mathbf{Z}/2\mathbf{Z})$$

de type $(3, \mathbf{Z}/2\mathbf{Z})$.

Plus généralement, la conjecture de Milnor peut être interprétée comme fournissant des invariants cohomologiques "supérieurs", chacun défini sur le noyau du précédent.

7.2. Le cas de $\mathbf{SL}_D$: invariant de Merkurjev-Suslin

Soit $\mathbf{SL}_D$ le groupe associé à une algèbre centrale simple D de rang n^2 sur F, cf. n° 5.4. Supposons n premier à la caractéristique de F. La théorie de Kummer permet alors d'identifier $H^1(F,\mu_n)$ à F^*/F^{*n} ; si $t \in F^*$, notons (t) l'élément correspondant de $H^1(F,\mu_n)$. Soit d'autre part (D) la classe de D dans le groupe de Brauer $\mathrm{Br}(F)$; comme $n(D) = 0$, (D) appartient au sous-groupe $H^2(F,\mu_n)$ de $\mathrm{Br}(F)$. Le cup-produit $(t)(D)$ est un élément de $H^3(F,\mu_n^{\otimes 2})$, et l'on vérifie facilement que l'on a $(t)(D) = 0$ si $t \in \mathrm{Nrd}(D^*)$. D'où, par passage au quotient, un homomorphisme

$$F^*/\mathrm{Nrd}(D^*) \longrightarrow H^3(F,\mu_n^{\otimes 2}).$$

Comme $F^*/\mathrm{Nrd}(D^*) = H^1(F,\mathbf{SL}_D)$, on a ainsi défini (après remplacement de F par une extension L quelconque...) un *invariant cohomologique de type* $(3,\mu_n^{\otimes 2})$ pour les $\mathbf{SL}_D$-torseurs. (Noter que, si n divise 24, on a $\mu_n^{\otimes 2} = \mathbf{Z}/n\mathbf{Z}$.)

Le cas le plus favorable est celui où n est sans facteur carré :

Théorème 8 (Merkurjev-Suslin [21], 12.2) – *Si n est sans facteur carré, l'application*

$$a : H^1(F,\mathbf{SL}_D) \longrightarrow H^3(F,\mu_n^{\otimes 2}),$$

définie ci-dessus, est injective.

Autrement dit, un élément t de F^* est norme réduite d'un élément de D^* si et seulement si $(t)(D) = 0$ dans $H^3(F,\mu_n^{\otimes 2})$.

Remarques

(1) Pour $n = 2$, D est une algèbre de quaternions, et $\mathbf{SL}_D$ s'identifie au groupe $\mathbf{Spin}(q)$ associé à une forme quadratique q de rang 3 ; l'invariant ci-dessus est égal à l'invariant d'Arason du n° 7.1.

(2) Si n a des facteurs carrés (par exemple $n = 4$), l'application a n'est pas injective en général : il faut trouver d'autres invariants...

7.3. Les invariants de Rost

Les exemples ci-dessus, ainsi que ceux des §§ 8,9, laissaient penser qu'il existe des invariants cohomologiques de type $(3,\mu_n^{\otimes 2})$ pour tout type de groupe simplement connexe (avec n dépendant du type de G, par exemple $n = 2,3,5$ pour G de type E_8, cf. [33], § 3). C'est effectivement ce que vient de démontrer Rost ([30]). Voici le principe de sa construction :

On suppose G absolument presque simple, simplement connexe, et F de caractéristique 0 (pour simplifier). Soit P un G-torseur sur une extension L de F. On se propose d'associer à P un élément $a(P)$ du groupe

$$H^3(L, \mathbf{Q}/\mathbf{Z}(2)) = \varinjlim H^3(L, \mu_n^{\otimes 2}).$$

(Noter que, en vertu d'un théorème de Merkurjev-Suslin (cf. [38], th. 21.4), les applications canoniques $H^3(L, \mu_n^{\otimes 2}) \to H^3(L, \mathbf{Q}/\mathbf{Z}(2))$ sont injectives ; on peut donc voir $H^3(L, \mathbf{Q}/\mathbf{Z}(2))$ comme la *réunion* des $H^3(L, \mu_n^{\otimes 2})$.)

Choisissons une extension finie L' de L qui déploie G, et sur laquelle P a un point rationnel. On a $P_{/L'} \simeq G_{/L'}$. Considérons le groupe de cohomologie étale $H^3_{\text{et}}(P_{/L'})$, à coefficients dans $\mathbf{Q}/\mathbf{Z}(2)$. Il n'est pas difficile de voir que ce groupe se décompose en somme directe :

$$H^3_{\text{et}}(P_{/L'}) = H^3(L') \oplus \mathbf{Q}/\mathbf{Z} \qquad (\text{avec } H^3(L') = H^3(L', \mathbf{Q}/\mathbf{Z}(2)),$$

où la projection sur le premier facteur est définie par le choix d'un point L'-rationnel de P (deux points différents donnant la même projection), et le second facteur est le groupe de cohomologie "géométrique", sur L_s. (Rappelons que ce dernier groupe est le même que sur $\mathbf{C}$; pour voir que c'est $\mathbf{Q}/\mathbf{Z}$, utiliser le fait que $\pi_2 = 0$ et $\pi_3 = \mathbf{Z}$.)

Notons u_P l'élément de $H^3_{\text{et}}(P_{/L'})$ dont les deux composantes sont respectivement 0 et $1/m$, avec $m = [L' : L]$. Considérons l'homomorphisme de *trace* (= image directe = corestriction)

$$\mathrm{Tr} : H^3_{\text{et}}(P_{/L'}) \longrightarrow H^3_{\text{et}}(P).$$

D'où un élément $v_P = \mathrm{Tr}(u_p)$ de $H^3_{\text{et}}(P)$. Or on a une suite exacte

$$0 \longrightarrow H^3(L) \longrightarrow H^3_{\text{et}}(P) \longrightarrow \mathbf{Q}/\mathbf{Z},$$

déduite de la suite spectrale reliant les cohomologies de P et de $P_{/L_s}$. L'image de v_P dans $\mathbf{Q}/\mathbf{Z}$ est $m.(1/m) = 0$; on a donc

$$v_P \in H^3(L) = H^3(L, \mathbf{Q}/\mathbf{Z}(2)).$$

On vérifie sans mal que v_P est indépendant du choix de L' ; *c'est l'invariant* $a(P)$ *cherché.*

Exemple. Si G est de type E_8, on montre, en utilisant le plongement de G dans $\mathbf{SL}_{248}$ donné par la représentation adjointe, que $60.a(P) = 0$. D'où un invariant cohomologique

$$H^3(L,G) \longrightarrow H^3(L,\mu_{60}^{\otimes 2}) = H^3(L,\mathbf{Z}/4\mathbf{Z}) \oplus H^3(L,\mathbf{Z}/3\mathbf{Z}) \oplus H^3(L,\mu_5^{\otimes 2}).$$

Rost montre en outre que "60" ne peut pas être amélioré : si P désigne le G-torseur *versel* associé(1) à un plongement de G dans un groupe $\mathbf{SL}_d$, l'invariant $a(P)$ de P *est d'ordre* 60. [Cette non trivialité de a se démontre en utilisant des sous-groupes bien choisis de E_8. Ainsi, pour prouver que la 5-composante de $a(P)$ n'est pas toujours nulle, on utilise des sous-groupes de G (supposé déployé) de type $A_4.A_4$, ou même des sous-groupes finis (non toriques) de type $\mu_5 \times \mu_5 \times \mathbf{Z}/5\mathbf{Z}$. De façon générale, il semble y avoir des relations entre les invariants cohomologiques de G, et ses sous-groupes abéliens élémentaires (pour une analyse de ceux-ci, voir Griess [11]).]

EXEMPLES : $\mathbf{G_2}$ ET $\mathbf{F_4}$

§ 8. LE CAS DE $\mathbf{G_2}$

On suppose F de caractéristique $\neq 2$ (sinon, voir n° 10.3). On écrit $H^i(F)$ pour $H^i(F,\mathbf{Z}/2\mathbf{Z})$. Si $t \in F^*$, on note (t) l'élément correspondant de $H^1(F)$, cf. n° 7.2. Le sous-ensemble de $H^i(F)$ formé des cup-produits $(t_1)\cdots(t_i)$, avec $t_1,\cdots,t_i \in F^*$, est noté $H^i_{\mathrm{dec}}(F)$; un élément de cet ensemble est dit *décomposable.*

(1) Rappelons, d'après Grothendieck [12], ce qu'est ce torseur. Si l'on choisit un plongement de G dans un groupe $\mathbf{SL}_d$, on définit L comme le corps des fonctions de la F-variété $X = \mathbf{SL}_d/G$. La fibre générique P de la projection $\mathbf{SL}_d \to X$ est un G-torseur défini sur L, qui est "versel" en ce sens que tout autre G-torseur s'en déduit par spécialisation (pour plus de précisions, voir [12]).

8.1. Description de $H^1(F,G)$, pour G de type G_2

Soit G un F-groupe simple de type G_2. On suppose que G est *déployé* (ce n'est pas une restriction : le cas général se ramène à celui-là par torsion, cf. n° 2.1).

Théorème 9 – *Il y a des bijections canoniques* (décrites ci-dessous) *entre* :
(i) $H^1(F,G)$;
(ii) $H^3_{\text{dec}}(F)$;
(iii) *l'ensemble des classes d'isomorphisme de F-formes de G* ;
(iv) *l'ensemble des classes d'isomorphisme d'algèbres d'octonions sur F* ;
(v) *l'ensemble des classes d'isomorphisme de 3-formes de Pfister sur F.*

(Rappelons qu'une 1-forme de Pfister est une forme quadratique binaire qui représente 1, i.e. qui s'écrit X^2+tY^2, et qu'une n-forme de Pfister est un produit tensoriel de n 1-formes de Pfister. Une 3-forme de Pfister peut donc s'écrire :

$$(*) \qquad X_0^2+t_1X_1^2+t_2X_2^2+t_3X_3^2+t_1t_2X_4^2+t_2t_3X_5^2+t_1t_3X_6^2+t_1t_2t_3X_7^2$$

avec $t_i \in F^*$.)

Les bijections (i) $\to$ (iii) et (i) $\to$ (iv) proviennent de ce que le groupe d'automorphismes de G (resp. d'une algèbre d'octonions déployée) est isomorphe à G. La bijection (iv) $\to$ (v) se définit en associant à une algèbre d'octonions C sa forme norme N_C, qui est une 3-forme de Pfister ; on sait (cf. par exemple [6], (2.3)) que N_C détermine C à isomorphisme près, et peut être choisie arbitrairement. La flèche (v) $\to$ (ii) s'obtient en associant à la 3-forme de Pfister $(*)$ son *invariant d'Arason* ([1], § 1), qui est $(-t_1)(-t_2)(-t_3)$, donc est décomposable. La surjectivité de cette flèche est claire. Son injectivité résulte d'un théorème de Merkurjev, cf. [2], prop. 2 (l'énoncé analogue pour les n-formes de Pfister est connu pour $n \leq 5$).

Remarque – La flèche $H^1(F,G) \to H^3(F)$ du th. 9 peut également se définir comme le composé

$$H^1(F,G) \longrightarrow H^1(F,\mathbf{Spin}_7) \xrightarrow{a} H^3(F),$$

où a est l'invariant du n° 7.1. C'est aussi un cas particulier des invariants de Rost (n° 7.3).

8.2. Exemples

Si $H^3(F) = 0$ (par exemple si $\mathrm{cd}_2(\Gamma_F) \leq 2$), le th. 9 montre que $H^1(F, G) = 0$; autrement dit toute algèbre d'octonions sur F est déployée, et tout groupe de type G_2 est déployé. Inversement, si $H^1(F, G) = 0$, on a $H^3(F) = 0$, d'après Merkurjev-Suslin ([21], th. 5.7).

Si $F = \mathbf{R}$, $H^3(F)$ a deux éléments : 0 et $(-1)(-1)(-1)$, qui correspondent respectivement à la forme déployée et à la forme compacte de G_2.

Si $F = k((T))$, avec $H^3(k) = 0$, on a $H^3(F) = H^2(k)$, et $H^3_{\text{dec}}(F) = H^2_{\text{dec}}(k)$. On voit ainsi que les algèbres d'octonions sur F correspondent aux algèbres de quaternions sur k, résultat qu'il est facile de démontrer directement (ou de déduire de la théorie de Bruhat-Tits [9], si k est parfait).

8.3. Un autre exemple (et un nouveau problème)

Soit k un corps p-adique, autrement dit une extension finie d'un corps $\mathbf{Q}_p$, p premier. Soit $F = k(T)$. On a $\mathrm{cd}_2(F) = 3$, et il n'est pas difficile de déterminer explicitement $H^3(F)$. Le résultat est le suivant :

Soit P l'ensemble des *points fermés* de la droite projective $\mathbf{P}_1$ sur k, autrement dit l'ensemble des valuations discrètes de F triviales sur k. Soit $C(P)$ le $\mathbf{F}_2$-espace vectoriel des *fonctions* $f : P \to \mathbf{Z}/2\mathbf{Z}$, *à support fini*, et *de somme nulle* (autrement dit, l'ensemble des parties finies paires de P, avec la loi d'addition $A + B = A \cup B - A \cap B$). Le groupe $H^3(F)$ *s'identifie* à $C(P)$. Cette identification se fait en associant à $x \in H^3(F)$ la fonction $f_x \in C(P)$ définie par :

$$f_x(v) = \text{image de } x \text{ dans } H^3(\widehat{F}_v) = \mathbf{Z}/2\mathbf{Z}, \text{ si } v \in P,$$

où $\widehat{F}_v$ est le complété de F en v (isomorphe à $k_v((T))$, où k_v est une extension finie de k). Que l'on obtienne ainsi un isomorphisme résulte de [1], 4.17, combiné avec le fait que la corestriction $H^2(k_v) \to H^2(k)$ est bijective.

Compte tenu du th. 9, on voit que $H^1(F, G)$ s'identifie à un sous-ensemble $C_{\text{dec}}(P)$ de $C(P)$; en termes plus concrets, on associe à une algèbre d'octonions sur F l'ensemble des $v \in P$ où cette algèbre "a mauvaise réduction" : c'est une partie finie paire de P. C'est satisfaisant... à cela près que l'on aimerait savoir ce qu'est le sous-ensemble $C_{\text{dec}}(P)$. *Est-il égal à* $C(P)$? Autrement dit, est-il vrai que *tout élément de* $H^3(F)$ *est décomposable* ? Ce serait vrai si tout forme quadratique à 9 variables sur F représentait 0 ; malheureusement, il ne semble pas que ce soit connu.

§ 9. LE CAS DE $\mathbf{F_4}$

On suppose F de caractéristique $\neq 2, 3$.

On note G un F-groupe simple déployé de type F_4.

9.1. Interprétations de $H^1(F,G)$

Ici encore, on a des bijections canoniques entre :

(i) $H^1(F,G)$;

(ii) l'ensemble des classes d'isomorphisme de F-formes de G ;

(iii) l'ensemble des classes d'isomorphisme d'algèbres de Jordan exceptionnelles sur F.

(Par "algèbre de Jordan exceptionnelle", on entend une algèbre de Jordan centrale simple de rang 27, du type considéré par Albert, cf. [15], [26], [35], [36].)

Comme l'ensemble $S(G)$ associé à G (cf. n° 2.2) est formé des nombres premiers 2 et 3, on s'attend à avoir des invariants cohomologiques mod 2 et mod 3. C'est bien le cas :

9.2. Invariants cohomologiques mod 2

Soit J une algèbre de Jordan exceptionnelle sur F. Associons-lui la "forme trace" correspondante, qui est une forme quadratique non dégénérée Q_J de rang 27 : $Q_J(x) = \frac{1}{2}\,\mathrm{Tr}(x^2)$, cf. [35], [36].

Théorème 10 (cf. [26], [29], [33]) – *Il existe une 3-forme de Pfister φ_3 et une 5-forme de Pfister φ_5 telles que l'on ait :*

$$Q_J \oplus \varphi_3 = \langle 2,2,2\rangle \oplus \varphi_5.$$

De plus, ces propriétés caractérisent φ_3 et φ_5 à isomorphisme près, et φ_5 est divisible par φ_3 (i.e. φ_5 est isomorphe au produit tensoriel de φ_3 par une 2-forme de Pfister).

(On a noté $\langle 2,2,2\rangle$ la forme quadratique ternaire $2X^2+2Y^2+2Z^2$.)

On traite d'abord le cas où J est *réduite*, i.e. possède un idempotent distinct de 0 et 1. On peut alors identifier J à une algèbre de matrices hermitiennes de type $(3,3)$ à coefficients dans une algèbre d'octonions ; la forme φ_3 est celle associée à l'algèbre d'octonions, et la formule

$$Q_J = \langle 2,2,2\rangle \oplus (\varphi_5 - \varphi_3)$$

se vérifie par un calcul direct (cf. [36], (32), p. 76). Le cas non réduit se ramène au cas réduit par extension de degré 3 du corps de base ; on utilise un théorème de descente pour les formes de Pfister démontré par Rost [29]. Pour une autre méthode, voir [26].

Les formes de Pfister φ_3 et φ_5 ont des *invariants d'Arason* ([1], § 1) qui appartiennent respectivement à $H^3_{\mathrm{dec}}(F,\mathbf{Z}/2\mathbf{Z})$ et $H^5_{\mathrm{dec}}(F,\mathbf{Z}/2\mathbf{Z})$, et qui les caractérisent. D'où des *invariants cohomologiques* mod 2 :

$$f_3 : H^1(F,G) \longrightarrow H^3(F,\mathbf{Z}/2\mathbf{Z}) \quad \text{et} \quad f_5 : H^1(F,G) \longrightarrow H^5(F,\mathbf{Z}/2\mathbf{Z}).$$

Remarque. Soit G_2^{dep} un groupe simple déployé de type G_2. Il y a un plongement naturel (défini à conjugaison près) $G_2^{\mathrm{dep}} \to G = F_4^{\mathrm{dep}}$ qui donne une application

$$H^1(F,G_2^{\mathrm{dep}}) \longrightarrow H^1(F,F_4^{\mathrm{dep}}).$$

L'invariant φ_3 donne une *rétraction canonique*

$$H^1(F,F_4^{\mathrm{dep}}) \longrightarrow H^1(F,G_2^{\mathrm{dep}}).$$

Il serait intéressant d'en avoir une définition plus directe.

9.3. Invariant cohomologique mod 3

A toute algèbre de Jordan exceptionnelle J sur F, Rost [28] associe un invariant :

$$g_3(J) \in H^3(F,\mathbf{Z}/3\mathbf{Z}) \qquad (\text{noter que } \mathbf{Z}/3\mathbf{Z} = \mu_3^{\otimes 2}).$$

L'une des façons de caractériser cet invariant est d'utiliser le fait que, si D est une algèbre centrale simple de rang 3^2, le groupe $\mathbf{SL}_D$ se plonge dans G. Cela donne une flèche $H^1(F, \mathbf{SL}_D) \to H^1(F, G)$; les éléments de $H^1(F, G)$ ainsi obtenus (pour un D convenable) correspondent aux algèbres de Jordan exceptionnelles fournies par la “première construction de Tits”. Le composé

$$H^1(F, \mathbf{SL}_D) \longrightarrow H^1(F, G) \xrightarrow{g_3} H^3(F, \mathbf{Z}/3\mathbf{Z})$$

coïncide avec l'invariant de Merkurjev-Suslin (n° 7.2) ; il n'est pas difficile de montrer que cette propriété *caractérise* l'invariant g_3 (c'est son *existence* qui n'est pas évidente).

Remarque – Les invariants f_3 et g_3 sont des cas particuliers des invariants du n° 7.3.

9.4. Utilisation des invariants f_3, f_5 et g_3

On peut se demander si la situation est aussi favorable pour F_4 que pour G_2. Autrement dit :

Question – *Est-il vrai qu'une algèbre de Jordan exceptionnelle J est déterminée à isomorphisme près par ses trois invariants $f_3(J)$, $f_5(J)$ et $g_3(J)$?*

On ne sait même pas répondre (autant que je sache) à la question suivante (cf. n° 2.4, Question 1) :

Si deux algèbres de Jordan exceptionnelles deviennent isomorphes sur une extension finie de F de degré premier à 6 (par exemple de degré 5) *sont-elles isomorphes* ?

Il y a toutefois des résultats partiels encourageants :

– J *est* réduite *si et seulement si* $g_3(J) = 0$.

– *Deux algèbres réduites sont isomorphes si et seulement si leurs invariants f_3 et f_5 sont égaux* (i.e. si leurs formes traces sont isomorphes, cf. [35], th. 1).

– *Une algèbre est* déployée *si et seulement si tous ses invariants sont* 0 (d'ailleurs la nullité de f_3 entraîne celle de f_5).

– *Soit* $F_4(J) = \mathrm{Aut}(J)$ *la F-forme de G associée à J. Pour que $F_4(J)$ soit* anisotrope, *il faut et il suffit que l'un des invariants $f_5(J)$ et $g_3(J)$ soit* $\neq 0$.

Une autre question naturelle est la détermination de *l'image* de l'application

$$H^1(F, G) \longrightarrow H^3(F, \mathbf{Z}/2\mathbf{Z}) \times H^5(F, \mathbf{Z}/2\mathbf{Z}) \times H^3(F, \mathbf{Z}/3\mathbf{Z}).$$

On a vu que les invariants f_3 et f_5 sont *décomposables*, et que l'invariant f_5 est divisible par l'invariant f_3 ; inversement, tout couple de classes de cohomologie satisfaisant à ces conditions est le système d'invariants d'une algèbre J, que l'on peut même supposer réduite (et qui est alors bien déterminée, à isomorphisme près). Quant à l'invariant g_3, Rost vient de prouver (non publié) qu'il est *décomposable* au sens suivant : c'est un cup-produit d'un élément de $H^1(F, \mathbf{Z}/3\mathbf{Z})$ et de deux éléments de $H^1(F, \mu_3)$; inversement, tout élément décomposable de $H^3(F, \mathbf{Z}/3\mathbf{Z})$ est l'invariant g_3 d'une algèbre fournie par la première construction de Tits. Reste la question : *quelles relations y a-t-il entre les invariants* $(\bmod 2)$ *et* $(\bmod 3)$? Le cas des corps de séries formelles (cf. [25]) montre que ces invariants ne sont pas indépendants (ce qu'indique aussi la théorie de Bruhat-Tits).

9.5. Un exemple

Reprenons les notations et hypothèses du n° 8.3 : $F = k(T)$, où k est un corps p-adique, et P est l'ensemble des points fermés de la droite projective sur k. Comme $\mathrm{cd}_2(\Gamma_F) = 3$, l'invariant f_5 est 0. On a vu que l'invariant f_3 peut être interprété comme une fonction $f : P \to \mathbf{Z}/2\mathbf{Z}$ à support fini, et de somme nulle. De même, g_3 s'interprète comme une fonction $g : P \to \mathbf{Z}/3\mathbf{Z}$ à support fini et de somme nulle. On peut prouver, en utilisant [25], que les supports de f et de g sont *disjoints* ; autrement dit, si l'on considère (f, g) comme une fonction $P \to \mathbf{Z}/6\mathbf{Z}$, *ses valeurs sont d'ordre* 1, 2 *ou* 3, *mais pas* 6. Y a-t-il d'autres relations entre f et g ?

CORPS IMPARFAITS

§ 10. LA p-COHOMOLOGIE D'UN CORPS DE CARACTÉRISTIQUE p

Supposons F de caractéristique $p > 0$. La p-cohomologie galoisienne de F est peu intéressante : on a $\mathrm{cd}_p(\Gamma_F) \leq 1$, comme on l'a vu au n° 4.3. Si l'on veut définir des invariants cohomologiques ressemblant à ceux des §§ 7,8,9, il est nécessaire de changer de point de vue. C'est ce que l'on va faire.

10.1. Les groupes $H_p^{i+1}(F)$

Soit $\Omega_{\mathbf{Z}}(F)$ le F-espace vectoriel des formes différentielles de la $\mathbf{Z}$-algèbre F, cf. Bourbaki A III.134. Si i est un entier ≥ 0, posons $\Omega^i = \wedge^i \Omega_{\mathbf{Z}}(F)$. La différentiation extérieure d applique Ω^{i-1} dans Ω^i. Il existe une application additive p-linéaire $\gamma : \Omega^i \to \Omega^i/d\Omega^{i-1}$, et une seule, telle que $\gamma(x\omega) = x^p\omega$, si ω est produit de i différentielles logarithmiques dy/y ("inverse de l'opération de Cartier"). *On pose* :

$$H_p^{i+1}(F) = \mathrm{Coker}(\gamma - 1 : \Omega^i \longrightarrow \Omega^i/d\Omega^{i-1}).$$

D'après Milne [23] et Kato [16], le groupe $H_p^{i+1}(F)$ ainsi défini est *l'analogue en caractéristique p du groupe $H^{i+1}(F, \mu_p^{\otimes i})$ en caractéristique $\neq p$.* (Cette analogie peut se préciser, grâce à la K-théorie, cf. [16].)

Exemples

(1) Pour $i = 0$, on a $\Omega^i = F$ et $\gamma - 1$ n'est autre que le classique

$$\wp : x \mapsto x^p - x$$

d'Artin-Schreier. D'où :

$$H_p^1(F) = F/\wp F = H^1(\Gamma_F, \mathbf{Z}/p\mathbf{Z}),$$

et l'on retrouve le H^1 galoisien.

(2) Pour $i = 1$, on peut montrer que $H_p^2(F)$ s'identifie au sous-groupe $\mathrm{Br}_p(F)$ de $\mathrm{Br}(F)$ formé des éléments annulés par p. (L'identification se fait en associant à une forme différentielle $\omega = xdy/y$, avec $y \in F^*$, l'algèbre centrale simple de rang p^2 définie par des générateurs X, Y liés par les relations $X^p - X = x$, $Y^p = y$, $YXY^{-1} = X + 1$.)

10.2. Exemple : formes de Pfister en caractéristique 2

On suppose que $p = 2$. Soit q une *$(i+1)$-forme de Pfister* sur F. Rappelons (cf. [3], [16]) que l'on peut écrire q comme produit tensoriel

$$(*) \qquad q = q_a \otimes \varphi_{b_1} \otimes \cdots \otimes \varphi_{b_i} \qquad (a \in F,\ b_1, \cdots, b_i \in F^*),$$

où q_a désigne la forme quadratique binaire $X^2 + XY + aY^2$, et φ_b est la forme symétrique bilinéaire binaire $X_1Y_1 + bX_2Y_2$. [Ces définitions ont un sens car le produit tensoriel d'une forme bilinéaire symétrique par une forme quadratique (resp. une forme bilinéaire symétrique) est une forme quadratique (resp. une forme bilinéaire symétrique).]

A une telle forme q, on associe :

$$a(q) = \text{image de } a(db_1/b_1) \wedge \cdots \wedge (db_i/b_i) \text{ dans } H_2^{i+1}(F).$$

On montre (cf. [16]) que $a(q)$ ne dépend pas de la décomposition $(*)$ choisie ; c'est donc un *invariant* de q, analogue à l'invariant d'Arason en caractéristique $\neq 2$. De plus, *deux formes de Pfister sont isomorphes si et seulement si leurs invariants sont égaux* (*loc. cit.*, prop. 3).

Ainsi, les classes de $(i+1)$-formes de Pfister correspondent bijectivement aux éléments *décomposables* de $H_2^{i+1}(F)$ (un élément de $H_2^{i+1}(F)$ est dit décomposable s'il est l'image d'une forme différentielle $x_0 dx_1 \wedge \cdots \wedge dx_i$).

10.3. Le cas de G_2 en caractéristique 2

Soit G un F-groupe simple déployé de type G_2 ; supposons F de caractéristique 2.

Théorème 11 – *Le th.* 9 *du n°* 8.1 *reste valable, à condition d'y remplacer* $H^3_{\mathrm{dec}}(F)$ *par le sous-ensemble de* $H^3_2(F)$ *formé des éléments décomposables au sens du n°* 10.2.

La démonstration est la même que celle du th. 9, compte tenu des résultats de Kato rappelés ci-dessus.

Corollaire – *On a* $H^1(F, G) = 0$ *si* F *est parfait, ou si* $[F : F^2] = 2$.

En effet, on a alors $\Omega^2 = 0$, d'où $H^3_2(F) = 0$.

Remarque. Il devrait y avoir des résultats analogues pour F_4 en caractéristique 2 et en caractéristique 3.

BIBLIOGRAPHIE

[1] J. ARASON - *Cohomologische Invarianten quadratischer Formen*, J. Algebra **36** (1975), 446-491.

[2] J. ARASON - *A proof of Merkurjev's theorem*, Canadian Math. Soc. Conference Proc. **4** (1984), 121-130.

[3] R. BAEZA - *Quadratic forms over semilocal rings*, Lect. Notes in Math. **655** (1978).

[4] E. BAYER-FLUCKIGER et H.W. LENSTRA, Jr. - *Forms in odd degree extensions and self-dual normal bases*, Amer. J. of Math. **112** (1990), 359-373.

[5] E. BAYER-FLUCKIGER et R. PARIMALA - *Galois cohomology of classical groups over fields of cohomological dimension* ≤ 2, en préparation.

[6] F. van der BLIJ et T.A. SPRINGER - *The arithmetics of octaves and of the group* G_2, Indag. Math. **21** (1959), 406-418.

[7] A. BOREL - *Oeuvres*, Vol. II (1959-1968), Springer-Verlag, 1983.

[8] A. BOREL et T.A. SPRINGER - *Rationality properties of linear algebraic groups* II, Tôhoku Math. J. **20** (1968), 443-497 (= A. Borel, *Oe.* 80).

[9] F. BRUHAT et J. TITS - *Groupes algébriques sur un corps local. Chap. III. Compléments et applications à la cohomologie galoisienne*, J. Fac. Sci. Univ. Tokyo **34** (1987), 671-698.

[10] V.I. CHERNOUSOV - *Le principe de Hasse pour les groupes de type* E_8 (en russe), Dokl. Akad. Nauk SSSR **306** (1989), 1059-1063 (trad. anglaise : Soviet Math. Dokl. **39** (1989), 592-596).

[11] R.L. GRIESS - *Elementary abelian p-subgroups of algebraic groups*, Geometriæ Dedicata **39** (1991), 253-305.

[12] A. GROTHENDIECK - *Torsion homologique et sections rationnelles*, Sém. Chevalley, *Anneaux de Chow et applications*, exposé 5, Paris, 1958.

[13] G. HARDER - *Über die Galoiskohomologie halbeinfacher Matrizengruppen* I, Math. Z. **90** (1965), 404-428 ; II, *ibid.*, **92** (1966), 396-415.

[14] G. HARDER - *Über die Galoiskohomologie halbeinfacher algebraischer Gruppen* III, J. Crelle **274/275** (1975), 125-138.

[15] N. JACOBSON - *Structure and Representations of Jordan Algebras*, A.M.S. Colloquium Publ. XXXIX, Providence, 1968.

[16] K. KATO - *Galois cohomology of complete discrete valuation fields*, Lect. Notes in Math. **967** (1982), 215-238.

[17] M. KNESER - *Galois-Kohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern* I, Math. Z. **88** (1965), 40-47 ; II, *ibid.*, **89** (1965), 250-272.

[18] M. KNESER - *Lectures on Galois Cohomology of Classical Groups*, Tata Inst. of Fund. Research, Bombay, 1969.

[19] R.E. KOTTWITZ - *Tamagawa numbers*, Ann. of Math. **127** (1988), 629-646.

[20] S. LANG - *Algebraic groups over finite fields*, Amer. J. of Math. **78** (1956), 555-563.

[21] A. S. MERKURJEV et A.A. SUSLIN - *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism* (en russe), Izv. Akad. Nauk SSSR **46** (1982), 1011-1046 (trad. anglaise : Math. USSR Izv. **21** (1983), 307-340).

[22] A. S. MERKURJEV et A.A. SUSLIN - *On the norm residue homomorphism of degree three*, LOMI preprint E-9-86, Leningrad, 1986.

[23] J.S. MILNE - *Duality in the flat cohomology of a surface*, Ann. Sci. E.N.S. **9** (1976), 171-202.

[24] J. MILNOR - *Algebraic K-theory and quadratic forms*, Invent. Math. **9** (1970), 318-344.

[25] H.P. PETERSSON - *Exceptional Jordan division algebras over a field with a discrete valuation*, J. Crelle **274/275** (1975), 1-20.

[26] H.P. PETERSSON et M.L. RACINE - *On the invariants* mod 2 *of Albert algebras*, à paraître.

[27] V. PLATONOV et A. RAPINCHUK - *Groupes algébriques et théorie des nombres* (en russe), ed. Nauka 1991 (trad. anglaise : *Algebraic Groups and Number Theory*, Acad. Press, Pure and Applied Math. vol. **139**, 1993).

[28] M. ROST - *A* (mod 3) *invariant for exceptional Jordan algebras*, C.R. Acad. Sci. Paris **313** (1991), 823-827.

[29] M. ROST - *A descent property for Pfister forms* (non publié), 1991.

[30] M. ROST - *Cohomology invariants*, en préparation.

[31] J.-P. SERRE - *Cohomologie galoisienne des groupes algébriques linéaires*, Colloque sur la théorie des groupes algébriques, Bruxelles (1962), 53-68 (= *Oe.* 53).

[32] J.-P. SERRE - *Cohomologie Galoisienne*, Lect. Notes in Math. **5** (1964) ; une nouvelle édition, révisée et complétée, paraîtra en décembre 1994.

[33] J.-P. SERRE - *Résumé de cours* 1990-1991, Annuaire du Collège de France, 1991, 111-121.

[34] T.A. SPRINGER - *Sur les formes quadratiques d'indice zéro*, C.R. Acad. Sci. Paris **234** (1952), 1517-1519.

[35] T.A. SPRINGER - *The classification of reduced exceptional simple Jordan algebras*, Indag. Math. **22** (1960), 414-422.

[36] T.A. SPRINGER - *Oktaven, Jordan-Algebren und Ausnahmegruppen*, notes polycopiées, Göttingen, 1963.

[37] R. STEINBERG - *Regular elements of semisimple algebraic groups*, Publ. Math. I.H.E.S. **25** (1965), 281-312.

[38] A.A. SUSLIN - *Algebraic K-theory and the norm-residue homomorphism*, J. Soviet Math. **30** (1985), 2556-2611.

[39] J. TITS - *Résumé de cours* 1990-1991, Annuaire du Collège de France, 1991, 125-137.

[40] J. TITS - *Sur les degrés des extensions de corps déployant les groupes algébriques simples*, C.R. Acad. Sci. Paris **315** (1992), 1131-1138.

Jean-Pierre SERRE

Collège de France
3, rue d'Ulm
F-75005 PARIS