Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le cours a été consacré au même sujet que celui de 1962-1963 : la *cohomologie galoisienne*. Il a surtout insisté sur les nombreux problèmes que posent les groupes semi-simples lorsque l'on ne fait pas d'hypothèse restrictive sur le corps de base.

§1. Notations

— k est un corps commutatif, supposé de caractéristique $\neq 2$, pour simplifier ;

— k_s est une clôture séparable de k ;

— $\mathrm{Gal}(k_s/k)$ est le groupe de Galois de k_s/k ; c'est un groupe profini.

Si G est un groupe algébrique sur k, on note $\mathrm{H}^1(k, \mathrm{G})$ le premier ensemble de cohomologie de $\mathrm{Gal}(k_s/k)$ à valeurs dans $\mathrm{G}(k_s)$, cf. *Cohomologie Galoisienne,* LN 5, p. I-56. C'est un ensemble pointé.

Si A est un $\mathrm{Gal}(k_s/k)$-module, on définit pour tout $n \geqslant 0$ des groupes de cohomologie $\mathrm{H}^n(k, \mathrm{A}) = \mathrm{H}^n(\mathrm{Gal}(k_s/k), \mathrm{A})$, cf. LN 5, p. I-9.

Par exemple, si $\mathrm{A} = \mathbf{Z}/2\mathbf{Z}$, on a

$\mathrm{H}^1(k, \mathbf{Z}/2\mathbf{Z}) = k^*/k^{*2}$

et

$\mathrm{H}^2(k, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Br}_2(k)$ (noyau de la multiplication par 2 dans le groupe de Brauer de k).

L'un des thèmes du cours a été d'expliciter les relations qui existent (ou qui pourraient exister) entre l'ensemble $\mathrm{H}^1(k, \mathrm{G})$, pour G semi-simple, et les groupes $\mathrm{H}^n(k, \mathrm{A})$ pour $\mathrm{A} = \mathbf{Z}/2\mathbf{Z}$ (ou $\mathbf{Z}/3\mathbf{Z}$, ou tout autre « petit » module sur $\mathrm{Gal}(k_s/k)$).

§2. Le cas orthogonal

C'est celui qui est le mieux compris, grâce à son interprétation en termes de classes de formes quadratiques :

Soit q une forme quadratique non dégénérée de rang $n \geq 1$ sur k, et soit $\mathbf{O}(q)$ le *groupe orthogonal* de q, vu comme groupe algébrique sur k. Si x est un élément de $H^1(k, \mathbf{O}(q))$, on peut *tordre* q par x et l'on obtient une autre forme quadratique q_x de même rang n que q. L'application $x \mapsto (q_x)$ définit une *bijection* de $H^1(k, \mathbf{O}(q))$ sur l'ensemble des *classes de formes quadratiques non dégénérées de rang n* sur k.

On a un résultat analogue pour la composante neutre $\mathbf{SO}(q)$ de $\mathbf{O}(q)$, à condition de se borner aux formes quadratiques ayant même discriminant que q.

Ainsi, tout *invariant* des classes de formes quadratiques peut être interprété comme une fonction sur l'ensemble de cohomologie $H^1(k, \mathbf{O}(q))$, ou sur l'ensemble $H^1(k, \mathbf{SO}(q))$.

2.1. *Exemples d'invariants : les classes de Stiefel-Whitney*

Ecrivons q comme somme directe orthogonale de formes de rang 1 :

$q = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \ldots \oplus \langle a_n \rangle = \langle a_1, a_2, \ldots, a_n \rangle$, avec $a_i \in k^*$.

Si m est un entier ≥ 0, on définit un élément $w_m(q)$ de $H^m(k, \mathbf{Z}/2\mathbf{Z})$ par la formule

$$(2.1.1) \quad w_m(q) = \sum_{i_1 < \ldots < i_m} (a_{i_1}) \ldots (a_{i_m}).$$

(On a noté (a) l'élément de $H^1(k, \mathbf{Z}/2\mathbf{Z})$ défini par $a \in k^*$; le produit $(a_{i_1}) \ldots (a_{i_m})$ est un cup-produit dans l'algèbre de cohomologie $H^*(k, \mathbf{Z}/2\mathbf{Z})$.)

On montre (A. Delzant, *C.R. Acad. Sci. Paris,* 255, 1962) que $w_m(q)$ ne dépend de la classe d'isomorphisme de q (et pas de la décomposition choisie) ; cela provient du fait bien connu que les relations entre formes quadratiques « résultent des relations en rang ≤ 2 ».

On dit que $w_m(q)$ est la m-ième *classe de Stiefel-Whitney* de q.

Remarques. 1) Les classes $w_1(q)$ et $w_2(q)$ ont des interprétations standard : discriminant, invariant de Hasse-Witt. Les $w_m(q)$, $m \geq 3$, sont moins intéressantes ; il y a avantage à les remplacer (dans la mesure du possible) par les invariants de la théorie de Milnor, cf. n° 2.3 ci-après.

2) La même méthode conduit à d'autres invariants. Ainsi, si n est pair ≥ 4 et si $q = \langle a_1, \ldots, a_n \rangle$ est tel que $w_1(q) = 0$ (autrement dit, $a_1 \ldots a_n$ est un carré), on peut montrer que l'élément $(a_1) \ldots (a_{n-1})$ de $H^{n-1}(k, \mathbf{Z}/2\mathbf{Z})$ est un *invariant* de la classe de q. Le cas $n = 4$ est particulièrement intéressant.

2.2. Comportement de $w_1(q)$ et $w_2(q)$ par torsion

Soit $x \in \mathrm{H}^1(k, \mathbf{O}(q))$. On associe à x des éléments

$\delta^1(x) \in \mathrm{H}^1(k, \mathbf{Z}/2\mathbf{Z})$ et $\delta^2(x) \in \mathrm{H}^2(k, \mathbf{Z}/2\mathbf{Z})$

de la façon suivante :

$\delta^1(x)$ est l'image de x dans $\mathrm{H}^1(k, \mathbf{Z}/2\mathbf{Z})$ par l'application déduite de l'homomorphisme det : $\mathbf{O}(q) \to \{\pm 1\} = \mathbf{Z}/2\mathbf{Z}$;

$\delta^2(x)$ est le cobord de x (LN 5, p. I-71) relatif à la suite exacte de groupes algébriques :

$$1 \to \mathbf{Z}/2\mathbf{Z} \to \tilde{\mathbf{O}}(q) \to \mathbf{O}(q) \to 1.$$

(Le groupe $\tilde{\mathbf{O}}(q)$ est un certain revêtement quadratique de $\mathbf{O}(q)$ qui prolonge le revêtement spinoriel $\mathbf{Spin}(q) \to \mathbf{SO}(q)$. On peut le caractériser par la propriété suivante : une symétrie par rapport à un vecteur de carré a se relève en un élément d'ordre 2 de $\tilde{\mathbf{O}}(q)$ rationnel sur le corps $k(\sqrt{a})$.)

Les invariants $\delta^1(x)$ et $\delta^2(x)$ permettent de calculer les classes w_1 et w_2 de la forme q_x déduite de q par torsion au moyen de x. On a en effet :

(2.2.1) $w_1(q_x) = w_1(q) + \delta^1(x)$ dans $\mathrm{H}^1(k, \mathbf{Z}/2\mathbf{Z})$,

(2.2.2) $w_2(q_x) = w_2(q) + \delta^1(x) \cdot w_1(q) + \delta^2(x)$ dans $\mathrm{H}^2(k, \mathbf{Z}/2\mathbf{Z})$.

2.3. Les conjectures de Milnor

Soit $\mathbf{k}^{\mathrm{M}}(k) = \oplus\, \mathbf{k}_n^{\mathrm{M}}(k)$ *l'anneau de Milnor* (mod 2) de k, défini au moyen de symboles multilinéaires $(a_1, \ldots, a_n) = (a_1) \ldots (a_n)$, $a_i \in k^*$, avec les relations $2(a) = 0$ et $(a,b) = 0$ si $a + b = 1$.

Soient W_k l'anneau de Witt de k, et I_k son idéal d'augmentation, noyau de l'homomorphisme canonique $\mathrm{W}_k \to \mathbf{Z}/2\mathbf{Z}$.

On définit de façon naturelle des homomorphismes

(2.3.1) $\mathbf{k}_n^{\mathrm{M}}(k) \to \mathrm{I}_k^n/\mathrm{I}_k^{n+1}$

et

(2.3.2) $\mathbf{k}_n^{\mathrm{M}}(k) \to \mathrm{H}^n(k, \mathbf{Z}/2\mathbf{Z})$.

Les conjectures de Milnor (*Invent. Math.* 9, 1970) disent que ces homomorphismes sont des *isomorphismes*. Cela a été démontré pour $n < 4$ (Merkurjev-Suslin, Arason, Rost) et il y a des résultats partiels pour $n \geqslant 4$.

Le cours s'est borné à citer ces énoncés sans en donner de démonstrations. Il a été complété par deux exposés de B. Kahn sur les formes de Pfister et leurs invariants cohomologiques.

§3. Applications et exemples

3.1. Invariants à valeurs dans $H^3(k, \mathbf{Z}/2\mathbf{Z})$: *le cas du groupe spinoriel*

Soit q une forme quadratique non dégénérée sur k, et soit x un élément de $H^1(k, \mathbf{Spin}(q))$. Si l'on tord q par x, on obtient une forme quadratique q_x de même rang que q. D'après (2.2.1) et (2.2.2), les invariants w_1 et w_2 de q_x sont les mêmes que ceux de q. Il en résulte que l'élément $q_x - q$ de l'anneau de Witt W_k appartient au cube I_k^3 de l'idéal d'augmentation I_k. En utilisant l'homomorphisme

$$I_k^3/I_k^4 \to H^3(k, \mathbf{Z}/2\mathbf{Z})$$

construit par Arason (qui est en fait un isomorphisme, cf. n° 2.3), on obtient un élément de $H^3(k, \mathbf{Z}/2\mathbf{Z})$ que nous noterons $i(x)$. On a :

(3.1.1) $\quad i(x) = 0 \iff q_x \equiv q \pmod{I_k^4}$.

On a ainsi défini une application canonique

(3.1.2) $\quad i : H^1(k, \mathbf{Spin}(q)) \to H^3(k, \mathbf{Z}/2\mathbf{Z})$.

3.2. Invariants à valeurs dans $H^3(k, \mathbf{Z}/2\mathbf{Z})$: *cas général*

Prenons pour G un groupe semi-simple *simplement connexe* déployé, et choisissons une représentation irréductible ρ de G dans un espace vectoriel V de dimension finie. Supposons ρ orthogonale, ce qui est par exemple le cas si G est de l'un des types G_2, F_4 ou E_8. Il existe alors une forme quadratique non dégénérée q sur V qui est invariante par $\rho(G)$. On obtient ainsi un homomorphisme $G \to \mathbf{O}(q)$. Vu les hypothèses faites sur G, cet homomorphisme se relève en un homomorphisme $\tilde{\rho} : G \to \mathbf{Spin}(q)$.

En utilisant (3.1.2) on déduit de là une application

(3.2.1) $\quad i_\rho : H^1(k, G) \to H^3(k, \mathbf{Z}/2\mathbf{Z})$,

dont on montre facilement qu'elle ne dépend pas du choix de q.

3.3. Le groupe G_2

Supposons que G soit de type exceptionnel G_2, et soit déployé. On sait qu'il y a alors des bijections naturelles entre les trois ensembles suivants :

$H^1(k, G_2)$;
classes d'algèbres d'octonions sur k ;
classes de 3-formes de Pfister sur k.

Il résulte de là, et des théorèmes cités ci-dessus, que, si l'on prend pour ρ la représentation fondamentale de degré 7 de G_2, l'application i_ρ correspondante est une *bijection de* $H^1(k, G_2)$ *sur le sous-ensemble de* $H^3(k, \mathbf{Z}/2\mathbf{Z})$ *formé des éléments décomposables* (cup-produits de trois éléments de $H^1(k, \mathbf{Z}/2\mathbf{Z})$).

Cela donne une description cohomologique tout à fait satisfaisante de l'ensemble $H^1(k, G_2)$.

On peut aller un peu plus loin. Notons i l'injection de $H^1(k, G_2)$ dans $H^3(k, \mathbf{Z}/2\mathbf{Z})$ que nous venons de définir. Soit ρ une représentation irréductible quelconque de G_2 ; il lui correspond d'après (3.2.1) une application

$i_\rho : H^1(k, G_2) \to H^3(k, \mathbf{Z}/2\mathbf{Z})$.

On désire comparer i_ρ à i. Le résultat est le suivant (je me borne ici au cas où le corps de base est de caractéristique 0) :

(3.3.1) *On a, soit* $i_\rho = i$, *soit* $i_\rho = 0$.

De façon plus précise, soit $m_1\omega_1 + m_2\omega_2$ le poids dominant de ρ, écrit comme combinaison linéaire des poids fondamentaux ω_1 et ω_2 (ω_1 correspondant à la représentation de degré 7, et ω_2 à la représentation adjointe). On peut déterminer (grâce à des formules qui m'ont été communiquées par J. Tits) dans quel cas on a $i_\rho = i$; on trouve que cela se produit si et seulement si le couple (m_1, m_2) est congru (mod 8) à l'un des douze couples suivants) :

(0,2), (0,3), (1,0), (1,4), (2,0), (2,3), (4,3), (4,6), (5,2), (5,6), (6,3), (6,4).

Ainsi, pour la représentation adjointe, qui correspond à (0,1), on a $i_\rho = 0$. On peut préciser ceci en déterminant explicitement la forme de Killing Kill_x de la k-forme de G_2 associée à un élément donné $x \in H^1(k, G_2)$. Si $q_x = \langle 1 \rangle \oplus q_x^\circ$ est la 3-forme de Pfister associée à x (i.e. la *forme norme* de l'algèbre d'octonions correspondante), on trouve que Kill_x *est isomorphe à* $\langle -1, -3 \rangle \otimes q_x^\circ$.

3.4 Le groupe F_4

Ici encore, on dispose d'une interprétation concrète de la cohomologie : les éléments de $H^1(k, F_4)$ correspondent aux classes d'*algèbres de Jordan simples exceptionnelles* de dimension 27 sur k. Malheureusement, on est loin de savoir classer de telles algèbres, malgré les nombreux résultats déjà obtenus par Albert, Jacobson, Tits, Springer, McCrimmon, Racine, Petersson... Ces résultats suggèrent que les éléments de $H^1(k, F_4)$ pourraient être caractérisés par deux types d'invariants :

(3.4.1 - « *invariant* mod 2 ») La classe de la forme bilinéaire « trace » associée à l'algèbre de Jordan, cette classe étant elle-même déterminée par le couple d'une 3-*forme de Pfister* et d'une 5-*forme de Pfister* divisible par la première. Du point de vue cohomologique, cela signifierait un élément décomposable $x_3 \in H^3(k, \mathbf{Z}/2\mathbf{Z})$ (obtenu par (3.2.1) grâce à la représentation irréductible ρ de dimension 26 de F_4), et un élément x_5 de $H^5(k, \mathbf{Z}/2\mathbf{Z})$ de la forme $x_5 = x_3yz$ avec $y, z \in H^1(k, \mathbf{Z}/2\mathbf{Z})$.

(3.4.2 - « *invariant* mod 3 ») Un élément de $H^3(k, \mathbf{Z}/3\mathbf{Z})$, dont je n'ai qu'une définition conjecturale, basée sur la « première construction de Tits » (on suppose ici que la caractéristique de k est $\neq 3$).

Pour le moment, le seul cas qui puisse être traité complètement est celui des algèbres de Jordan dites « réduites » (celles où l'invariant mod 3 est 0) : on sait, d'après un théorème de Springer, que l'invariant mod 2 (i.e. la forme trace) détermine alors l'algèbre de Jordan à isomorphisme près.

3.5. Le groupe E_8

Lorsque k est un corps de nombres, la structure de $H^1(k, E_8)$ vient d'être déterminée par Chernousov et Premet : le principe de Hasse est valable, ce qui entraîne par exemple que le nombre d'éléments de $H^1(k, E_8)$ est 3^r, où r est le nombre de places réelles de k. La démonstration de ce résultat a fait l'objet d'une série d'exposés dans le séminaire commun avec la chaire de Théorie des Groupes.

Lorsque k est un corps quelconque (ou même, par exemple, le corps $\mathbf{Q}(T)$), on sait fort peu de choses sur $H^1(k, E_8)$. Les résultats généraux de Grothendieck (*sém. Chevalley,* 1958) et de Bruhat-Tits (*J. Fac. Sci. Tokyo* 34, 1987) suggèrent qu'un élément de cet ensemble pourrait avoir comme invariants des classes de cohomologie (de dimension $\geqslant 3$) mod 2, mod 3 et mod 5 (car 2,3,5 sont les *nombres premiers de torsion* de E_8, cf. A. Borel, *Oe.* II, p. 776). J'ignore comment ces invariants pourraient être définis ; je ne sais même pas si les applications $i_p : H^1(k, E_8) \to H^3(k, \mathbf{Z}/2\mathbf{Z})$ du n° 3.2 peuvent être non triviales.

§4. Problèmes d'injectivité

L'ensemble $H^1(k, G)$ est fonctoriel en k et G :

a) Si k' est une extension de k, on a une application naturelle

$$H^1(k, G) \to H^1(k', G).$$

b) Si $G \to G'$ est un morphisme de groupes algébriques, on a une application naturelle $H^1(k, G) \to H^1(k, G')$.

On dispose d'une série de cas où ces applications sont *injectives* :

(4.1) - *(théorème de simplification de Witt)* - Si $q = q_1 \oplus q_2$, où les q_i sont des formes quadratiques, l'application $H^1(k, \mathbf{O}(q_1)) \to H^1(k, \mathbf{O}(q))$ est injective

(4.2) - Même énoncé, pour les *groupes unitaires* associés aux algèbres à involution sur k.

Ce résultat, nettement plus délicat que le précédent, a fait l'objet d'un exposé par E. Bayer.

(4.3) (Springer) - Injectivité de $H^1(k, \mathbf{O}(q)) \to H^1(k', \mathbf{O}(q))$ lorsque k' est une extension finie de k *de degré impair.*

(4.4) (Bayer-Lenstra) - Même énoncé que (4.3), pour les *groupes unitaires* au lieu des groupes orthogonaux.

(4.5) (Pfister) - Injectivité de $H^1(k, \mathbf{O}(q)) \to H^1(k, \mathbf{O}(q \otimes q'))$ lorsque le rang de q' est impair (le morphisme $\mathbf{O}(q) \to \mathbf{O}(q \otimes q')$ étant défini par le produit tensoriel).

On aimerait avoir d'autres énoncés du même type, par exemple les suivants (qui sont peut-être trop optimistes) :

(4.6 ?) - Si k' est une extension finie de k de degré premier à 2 et 3, l'application $H^1(k, F_4) \to H^1(k', F_4)$ est injective.

(4.7 ?) - Même énoncé pour E_8, avec $\{2,3\}$ remplacé par $\{2,3,5\}$.

Remarque - Soit G un groupe algébrique sur k, et soient x,y deux éléments de $H^1(k, G)$. Supposons que x et y aient même images dans $H^1(k', G)$ et dans $H^1(k'', G)$ où k' et k'' sont deux extensions finies de k de degrés premiers entre eux (par exemple $[k' : k] = 2$ et $[k'' : k] = 3$). *Ceci n'entraîne pas* $x = y$ contrairement à ce qui se passe dans le cas abélien ; on peut en construire des exemples, en prenant G non connexe ; j'ignore ce qu'il en est lorsque G est connexe.

§5. Les formes traces

Il s'agit de la structure de la forme quadratique $\mathrm{Tr}(x^2)$ associée à une k-algèbre de dimension finie. Deux cas particuliers ont été considérés :

5.1. Algèbres centrales simples

Soit A une telle algèbre, supposée de degré fini n^2 sur k. On lui associe la forme quadratique q_A définie par

$q_A(x) = \mathrm{Trd}_{A/k}(x^2)$.

Notons q_A° la forme trace associée à l'algèbre de matrices $\mathbf{M}_n(k)$ de même rang que A ; c'est la somme directe d'une forme hyperbolique de rang $n(n-1)$ et d'une forme unité $\langle 1, 1, \ldots, 1\rangle$ de rang n.

On désire comparer q_A et q_A°. Il y a deux cas à distinguer :

(5.1.1) *n est impair.*

Les formes q_A et q_A° sont alors isomorphes ; cela résulte du théorème de Springer cité en (4.3).

(5.1.2) *n est pair.*

Soit (A) la classe de A dans le groupe de Brauer de k. Le produit de (A) par l'entier $n/2$ est un élément a de $\mathrm{Br}_2(k) = \mathrm{H}^2(k, \mathbf{Z}/2\mathbf{Z})$. On a :

$$w_1(q_A) = w_1(q^\circ_A) \qquad \text{et} \qquad w_2(q_A) = w_2(q^\circ_A) + a.$$

(La formule relative à w_1 est facile. Celle relative à w_2 s'obtient en considérant l'homomorphisme $\mathbf{PGL}_n \to \mathbf{SO}_{n^2}$ donné par la représentation adjointe et en montrant, par un calcul de poids et racines, que cet homomorphisme ne se relève pas au groupe $\mathbf{Spin}_{n^2}$ si n est pair).

5.2. *Algèbres commutatives étales*

Soit E une telle algèbre, soit n son rang et soit q_E la forme trace correspondante. Les invariants w_1 et w_2 de q_E sont donnés par une formule connue *(Comm. Math. Helv.* 59, 1984). Le cours a donné une démonstration de cette formule quelque peu différente de la démonstration originale, et a appliqué le résultat obtenu aux équations quintiques à la Kronecker-Hermite-Klein.

Le cas où le rang n de E est égal à 6 pose également des problèmes intéressants. Notons $e : \mathrm{Gal}(k_s/k) \to \mathrm{S}_6$ l'homomorphisme qui correspond à E par la théorie de Galois. En composant e avec un automorphisme extérieur de S_6 on obtient un homomorphisme $e' : \mathrm{Gal}(k_s/k) \to \mathrm{S}_6$ qui correspond à une autre algèbre étale E′ de rang 6 (« résolvante sextique »). *Peut-on déterminer $q_{E'}$, à partir de q_E ?* C'est vrai lorsque $w_1(q_E) = 0$, autrement dit lorsque les images de e et e' sont contenues dans le groupe alterné A_6 ; on peut en effet prouver que l'on a dans ce cas $q_{E'} \simeq 2q_E$ (mais pas $q_{E'} \simeq q_E$ en général, bien que q_E et $q_{E'}$ aient les mêmes invariants w_1 et w_2). Lorsque l'on a à la fois $w_1(q_E) = 0$ et $w_2(q_E) = 0$, on peut se demander si q_E est isomorphe à la forme unité $\langle 1, 1, \ldots, 1\rangle$. C'est vrai si k est un corps de nombres (ou un corps de fonctions rationnelles sur un corps de nombres) ; c'est faux en général : on peut construire un contre-exemple.

§6. La théorie de Bayer-Lenstra : les bases normales autoduales

Soit G un groupe fini. On s'intéresse aux G-*algèbres galoisiennes* sur k, ou, ce qui revient au même, aux G-*torseurs* sur k, G étant considéré comme un groupe algébrique de dimension 0 sur k. Une telle algèbre L est déterminée, à isomorphisme (non unique) près, par la donnée d'un homomorphisme continu $\varphi_L : \mathrm{Gal}(k_s/k) \to \mathrm{G}$, défini à conjugaison près.

Lorsque φ_L est surjectif, L est un corps, et c'est une extension galoisienne de k de groupe de Galois isomorphe à G.

Dans un travail récent (*Amer. J. Math.* 112, 1990), E. Bayer et H. Lenstra s'intéressent au cas où L possède une *base normale autoduale* (« BNA ») ; cela signifie qu'il existe un élément x de L tel que $q_L(x) = 1$ et que x soit orthogonal (relativement à q_L) à tous les gx, $g \in G$, $g \neq 1$. (Ainsi, les gx forment une « base normale » de L, et cette base est sa propre duale relativement à q_L.)

On peut donner un critère cohomologique pour l'existence d'une BNA : si U_G désigne le groupe unitaire de l'algèbre à involution $k[G]$, on a un plongement canonique de G dans $U_G(k)$; en composant φ_L avec ce plongement on obtient un homomorphisme $\mathrm{Gal}(k_s/k) \to U_G(k)$, homomorphisme que l'on peut regarder comme un 1-cocycle de $\mathrm{Gal}(k_s/k)$ à valeurs dans $U_G(k_s)$. La classe ε_L de ce cocycle est un élément de $H^1(k, U_G)$. *On a* $\varepsilon_L = 0$ *si et seulement si* L *a une* BNA.

De ce critère, combiné avec (4.4), Bayer-Lenstra déduisent le théorème suivant :

(6.1) - *S'il existe une extension de degré impair de k sur laquelle* L *acquiert une* BNA, *alors* L *a une* BNA *sur k.*

En particulier :

(6.2) - *Si* G *est d'ordre impair, toute* G*-algèbre galoisienne a une* BNA.

Voici quelques autres résultats relatifs aux BNA ; les démonstrations seront publiées en collaboration avec E. Bayer.

Soit L une G-algèbre galoisienne, et soit $\varphi_L : \mathrm{Gal}(k_s/k) \to G$ l'homomorphisme correspondant. Si x est un élément de $H^n(G, \mathbf{Z}/2\mathbf{Z})$, son image par $\varphi_L^* : H^n(G, \mathbf{Z}/2\mathbf{Z}) \to H^n(\mathrm{Gal}(k_s/k), \mathbf{Z}/2\mathbf{Z}) = H^n(k, \mathbf{Z}/2\mathbf{Z})$ sera notée x_L.

(6.3) - *Pour que* L *ait une* BNA, *il faut que* $x_L = 0$ *pour tout élément x de* $H^1(G, \mathbf{Z}/2\mathbf{Z})$ (autrement dit, l'image de $\mathrm{Gal}(k_s/k)$ dans G doit être contenue dans tous les sous-groupes d'indice 2 de G). *Cette condition est suffisante si la 2-dimension cohomologique de* $\mathrm{Gal}(k_s/k)$ *est* $\leqslant 1$ (autrement dit si les 2-sous-groupes de Sylow de $\mathrm{Gal}(k_s/k)$ sont des pro-2-groupes libres).

(6.4) - *Supposons que k soit un corps de nombres. Pour que* L *ait une* BNA, *il faut que* $\varphi_L(c_v) = 1$ *pour toute place réelle v de k* (c_v désignant la conjugaison complexe relative à une extension de v à k_s). *Cette condition est suffisante si* $H^1(G, \mathbf{Z}/2\mathbf{Z}) = H^2(G, \mathbf{Z}/2\mathbf{Z}) = 0$.

(6.5) - *Le cas où un 2-groupe de Sylow de* G *est abélien élémentaire.*

Soit S un 2-sous-groupe de Sylow de G. Supposons que S soit un groupe abélien élémentaire d'ordre 2^r, $r \geqslant 1$; l'ordre de G est $2^r m$, avec m impair.

(6.5.1) - *Il existe une r-forme de Pfister* q_L^1, *et une seule à isomorphisme près, telle que* $2^r q_L \simeq m \otimes q_L^1$ (somme directe de m copies de q_L^1).

Cette forme constitue un *invariant* de l'algèbre galoisienne L considérée. C'est la forme unité si L a une BNA. Réciproquement :

(6.5.2) - *Supposons que le normalisateur* N *de* S *opère transitivement sur* $S - \{1\}$. *Il y a alors équivalence entre* :

(i) L *a une* BNA.

(ii) *La forme* q_L *est isomorphe à la forme unité de rang* $2^r m$.

(iii) *La forme* q_L^1 *est isomorphe à la forme unité de rang* 2^r.

Lorsque r est assez petit, ce résultat peut se traduire en termes cohomologiques. En effet, on peut montrer qu'il existe un élément x de $H^r(G, \mathbf{Z}/2\mathbf{Z})$ dont la restriction à tout sous-groupe d'ordre 2 de G est $\neq 0$, et qu'un tel élément est unique, à l'addition près d'une classe de cohomologie « négligeable » (cf. §7 ci-après). L'élément correspondant x_L de $H^r(k, \mathbf{Z}/2\mathbf{Z})$ est un invariant de l'algèbre galoisienne L.

(6.5.3) - *Supposons* $r \leqslant 4$. *Les conditions* (i), (ii), (iii) *de* (6.5.2) *sont alors équivalentes à* :

(iv) *On a* $x_L = 0$ *dans* $H^r(k, \mathbf{Z}/2\mathbf{Z})$.

L'hypothèse $r \leqslant 4$ pourrait être supprimée si les conjectures du n° 2.3 étaient démontrées.

Exemples. 1) Supposons que $r = 2$ et que N opère transitivement sur $S - \{1\}$; c'est le cas si $G = A_4$, A_5 ou $\mathbf{PSL}_2(\mathbf{F}_q)$ avec $q \equiv 3 \pmod 8$. Le groupe $H^2(G, \mathbf{Z}/2\mathbf{Z})$ contient un seul élément $x \neq 0$; soit $\tilde{G}$ l'extension correspondante de G par $\mathbf{Z}/2\mathbf{Z}$. Il résulte de (6.5.3) que L *a une* BNA *si et seulement si l'homomorphisme* $\varphi_L : \mathrm{Gal}(k_s/k) \to G$ *se relève en un homomorphisme dans* $\tilde{G}$. Un tel relèvement correspond à une $\tilde{G}$-algèbre galoisienne $\tilde{L}$; on peut montrer qu'il est possible de s'arranger pour que $\tilde{L}$ possède elle aussi une BNA.

2) Prenons pour G le groupe $\mathbf{SL}_2(\mathbf{F}_8)$ ou le groupe de Janko J_1. Les hypothèses de (6.5.2) et (6.5.3) sont alors satisfaites avec $r = 3$. Le groupe $H^3(G, \mathbf{Z}/2\mathbf{Z})$ contient un seul élément $x \neq 0$, et l'on voit que L *a une* BNA *si et seulement si* $x_L = 0$ *dans* $H^3(k, \mathbf{Z}/2\mathbf{Z})$.

Remarque - La propriété pour une G-algèbre galoisienne L d'avoir une BNA peut se traduire en terme de « torsion galoisienne » de la manière suivante :

Soit V un espace vectoriel de dimension finie sur k, muni d'une famille $\mathbf{q} = (q_i)$ de *tenseurs quadratiques* (de type (2,0), (1,1), ou (0,2), peu importe). Supposons que G opère sur V en fixant chacun des q_i. On peut alors *tordre* $(V,\mathbf{q})$ par le G-torseur correspondant à L. On obtient ainsi une *k-forme* $(V,\mathbf{q})_L$ de $(V,\mathbf{q})$. On peut démontrer :

(6.6) - *Si* L *a une* BNA, $(V,\mathbf{q})_L$ *est isomorphe à* $(V,\mathbf{q})$.

De plus, cette propriété *caractérise* les algèbres galoisiennes ayant une BNA.

(Noter que ce résultat serait faux pour les tenseurs cubiques.)

§7. Classes de cohomologie négligeables

Soient G un groupe fini et A un G-module. Un élément x de $H^n(G, A)$ est dit *négligeable* (du point de vue galoisien) si, pour tout corps k, et tout homomorphisme continu $\varphi : \mathrm{Gal}(k_s/k) \to G$, on a

$\varphi^*(x) = 0$ dans $H^n(k, A)$.

Il revient au même de dire que $x_L = 0$ pour toute G-algèbre galoisienne L.

Exemple - Si a,b sont deux éléments quelconques de $H^1(G, \mathbf{Z}/2\mathbf{Z})$, le cup-produit $ab(a+b)$ est un élément négligeable de $H^3(G, \mathbf{Z}/2\mathbf{Z})$.

Voici quelques résultats sur ces classes :

(7.1) - *Pour tout groupe fini* G, *il existe un entier* N(G) *tel que toute classe de cohomologie d'ordre impair et de dimension* $n >$ N(G) *soit négligeable.*

Ce résultat ne subsiste pas pour les classes d'ordre pair. D'ailleurs aucune classe de cohomologie (à part 0) d'un groupe cyclique d'ordre 2 n'est négligeable, comme on le voit en prenant $k = \mathbf{R}$.

(7.2) - *Supposons* G *abélien élémentaire d'ordre* 2^r. *Si* $x \in H^n(G, \mathbf{Z}/2\mathbf{Z})$, *les propriétés suivantes sont équivalentes* :

(a) x *est négligeable.*

(b) *La restriction de* x *à tout sous-groupe d'ordre* 2 *de* G *est* 0.

(c) x *appartient à l'idéal de l'algèbre* $H^*(G, \mathbf{Z}/2\mathbf{Z})$ *engendré par les* $ab(a+b)$, *où* a *et* b *parcourent* $H^1(G, \mathbf{Z}/2\mathbf{Z})$.

Il y a des résultats analogues pour $A = \mathbf{Z}/p\mathbf{Z}$, avec p premier $\neq 2$.

SÉMINAIRES

B. KAHN, *Formes de Pfister et invariants cohomologiques* (2 exposés).

E. BAYER-FLUCKIGER, *Le théorème de simplification dans le cas hermitien.*

SÉMINAIRE COMMUN AVEC LA CHAIRE DE THÉORIE DES GROUPES

J.-P. SERRE, *Travaux de Chernousov sur les groupes de type* E_8.

J. TITS, *Travaux de Chernousov sur les groupes de type* E_8 (2 exposés).

J.-P. SERRE, *Remarques sur la cohomologie galoisienne des groupes semi-simples.*

PUBLICATIONS

J.-P. SERRE, *Construction de revêtements étales de la droite affine en caractéristique p* (*C.R. Acad. Sci. Paris,* 311, 1990, série I, 341-346).

— *Spécialisation des éléments de* $\mathrm{Br}_2(\mathbf{Q}(T_1, \ldots, T_n))$ (*C.R. Acad. Sci. Paris,* 311, 1990, série I, 397-402).

— *Relèvements dans* $\tilde{A}_n$ (*C.R. Acad. Sci. Paris,* 311, 1990, série I, 477-482).

— *Revêtements à ramification impaire et thêta-caractéristiques* (*C.R. Acad. Sci. Paris,* 311, 1990, série I, 547-552).

— *Les petits cousins* (*Miscellanea Mathematica,* Springer-Verlag, 1991, 277-291).

MISSIONS

Cours

— *Topics in Galois cohomology,* Harvard, septembre-décembre 1990.

— *Sieves,* Singapour, mai 1991.

Exposés

— *How often does a conic have a rational point ?,* State College, septembre 1990 ; Yale, novembre 1990.

— *Coverings of algebraic curves,* Harvard, octobre 1990.

— *Motives,* Harvard, octobre 1990.

— *Riemann Hypothesis : Why ?,* Chicago, octobre 1990.

— *Galois groups of division points of abelian varieties,* Chicago, octobre 1990.

— *Bounds for number of points of hypersurfaces over finite fields,* Chicago, octobre 1990.

— *Coverings with odd ramification and theta-characteristics,* Harvard, novembre 1990.

— *A chapter in group theory,* Yale, novembre 1990.

— *Asymptotic properties of the eigenvalues of some regular graphs,* Harvard, décembre 1990.

— *Prime numbers, Galois groups and* L*-functions* (3 exposés), Brown, décembre 1990.

— *Répartitions asymptotiques de valeurs propres de graphes et d'opérateurs de Hecke,* Bordeaux, février 1991 ; Univ. Paris VII, février 1991.

— *Nombres premiers, groupes de Galois, etc.* (2 exposés), E.N.S. Paris, mai 1991.

— *Motifs : une introduction,* E.N.S. Paris, mai 1991.

— *Galois cohomology : recent results and open questions,* Bonn, juin 1991.

— *Nombre de points de certaines surfaces* K3*, d'après Peters, Top et van der Vlugt,* Marseille-Luminy, juin 1991.