JEAN-PIERRE SERRE
E. BAYER (réd.)
C. GOLDSTEIN (réd.)

Quelques problèmes de cohomologie galoisienne

Cours de Jean-Pierre Serre, tome 12 (1991)
<http://www.numdam.org/item?id=CJPS_1991__12_>

Quelques problèmes de cohomologie galoisienne

J.-P. Serre

Collège de France, janvier-avril 1991

—

Notes de E. Bayer et C. Goldstein —

Annuaire du Collège de France

Résumé des cours 1990-1991

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 $n \geqslant 1$ sur k, et soit $\mathbf{O}(q)$ le *groupe orthogonal* de q, vu comme groupe algébrique sur k. Si x est un élément de $\mathrm{H}^1(k, \mathbf{O}(q))$, 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 $\mathrm{H}^1(k, \mathbf{O}(q))$ 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 $\mathrm{H}^1(k, \mathbf{O}(q))$, ou sur l'ensemble $\mathrm{H}^1(k, \mathbf{SO}(q))$.

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

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

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

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

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

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

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 $\leqslant 2$ ».

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 $w_m(q)$, $m \geqslant 3$, 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 $\geqslant 4$ et si $q = \langle a_1, \dots, a_n \rangle$ est tel que $w_1(q) = 0$ (autrement dit, $a_1 \dots a_n$ est un carré), on peut montrer que l'élément $(a_1) \dots (a_{n-1})$ de $\mathrm{H}^{n-1}(k, \mathbf{Z}/2\mathbf{Z})$ 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

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

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

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

2.3. Les conjectures de Milnor

Soit $\mathbf{k}^{\mathrm{M}}(k) = \oplus\, \mathbf{k}^{\mathrm{M}}_n(k)$ *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) $\quad \mathbf{k}^{\mathrm{M}}_n(k) \to \mathrm{I}^n_k/\mathrm{I}^{n+1}_k$

et

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

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 $i_\rho : H^1(k, E_8) \to H^3(k, \mathbf{Z}/2\mathbf{Z})$ 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 $\langle 1, 1, ..., 1\rangle$ 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 :

$$w_1(q_{\mathrm{A}}) = w_1(q^{\circ}_{\mathrm{A}}) \quad \text{et} \quad w_2(q_{\mathrm{A}}) = w_2(q^{\circ}_{\mathrm{A}}) + a.$$

(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 $q_{\mathrm{E}'}$, à partir de q_{E}* ? C'est vrai lorsque $w_1(q_{\mathrm{E}}) = 0$, 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 $q_{\mathrm{E}'} \simeq 2q_{\mathrm{E}}$ (mais pas $q_{\mathrm{E}'} \simeq q_{\mathrm{E}}$ en général, bien que q_{E} et $q_{\mathrm{E}'}$ aient les mêmes invariants w_1 et w_2). Lorsque l'on a à la fois $w_1(q_{\mathrm{E}}) = 0$ et $w_2(q_{\mathrm{E}}) = 0$, 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 $\varphi_{\mathrm{L}} : \mathrm{Gal}(k_s/k) \to \mathrm{G}$, 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* $Br_2(Q(T_1, \ldots, T_n))$ (*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.

Table

J-P. Serre

Cohomologie galoisienne

LN 5, Coh. Gal. (62-63), 1964
Supposé connu.

Cas particuliers concernant les formes quadratiques
groupes orthogonaux, groupes unitaires :
Bayer-Lenstra
Corps de fonctions $\mathbb{Q}(T)$

Rappel de définitions

K corps, $\overline{K}$ clôture algébrique

$\overline{K}$
|
K_s clôture separable
|
K

$G_K = \mathrm{Gal}(K_s/K)$ groupe profini
$= \varprojlim$ groupes finis.

1er contexte

A groupe abélien où opère G_K (continuement)
(fixateur dans G_K d'un élément de A est ouvert).

G_K-module.

On définit $H^i(G_K, A) = \varinjlim_{U} H^i(G_K/U, A^U)$

U s/g ouvert normal de G_K

H^i : foncteurs dérivés du foncteur "points fixes"

[illegible] du complexe des cochaînes

$f(g_1, \dots, g_i)$

$$\delta f(g_1, \dots, g_{i+1}) = g_1 f(g_2, \dots, g_{i+1}) - f(g_1 g_2, \dots, g_{i+1}) + \dots \pm f(g_1, \dots, g_i).$$

2ème situation A groupe, A non nécessairement commutatif où opère G_K

$H^0(G_K, A) = A^G$ (invariants) groupe

$H^1(G_K, A) = \varinjlim H^1(G_K/U, A^U)$

G groupe qui opère sur A

1-cocycle $s \in G \longmapsto a_s \in A$

$$a_{st} = a_s\, s(a_t) = a_s\, {}^s a_t \qquad s, t \in G$$

2 cocycles (a_s), (a'_s) sont cohomologues s'il existe $a \in A$ avec $a'_s = a^{-1} a_s\, {}^s a$ pour tout $s \in G$.

$H^1(G, A) = (\text{cocycles}) / \sim$ cob.

c'est un ensemble pointé.

Petit historique

Brauer ~ 1929 dans 2 contextes différents :

alg. centrales simples (groupe de Brauer)

$H^2(G_K, K_s^*) = Br(K)$

via représentations linéaires de groupes

Soit Γ un groupe fini

K corps (car. 0) $\subset \mathbb{C}$

ρ repr. irréd. / $\mathbb{C}$ de Γ

caractère à valeurs dans K

Peut-on la réaliser sur K ?

Sinon, pourquoi ?

ρ isom. aux ${}^s\rho$, $s \in G_K$

$${}^s\rho = A_s^{-1} \rho A_s$$

Est-ce que

$$A_{st} = A_s {}^s A_t \ ?$$

Si oui, on peut remplacer ρ par

ρ' tel que ${}^s\rho' = \rho'$.

Ce n'est pas tout à fait vrai, mais

on a $c_{st} A_{st} = A_s {}^s A_t \quad c_{st} \in K_s^*$

c_{st} est un 2-cocycle.

Sa classe dans H^2 est obstruction au problème.

Notation: $H^2(G_K, K_s^*) = H^2(K, \mathbb{G}_m)$

<u>Teichmüller</u> ~ 1940

L extension galoisienne finie

$\mid G$

K $\quad Br(K) \longrightarrow Br(L)^G$ surjectif ?

L'obstruction est un 3-cocycle : plus précisément un élément de $H^3(G, L^*)$ à image 0 dans $H^3(G_K, G_m)$.

descente et torsion : variétés de Severi-Brauer

Weil 1951 corps de classes sous forme cohomologique

Artin-Tate

Weil 1956 critère de descente du corps de base, cas galoisien ou transcendant

"Torsion galoisienne"

Généralisée ~~Développée~~ par Grothendieck : descente générale ~ 1958

topologie étale

Application aux groupes semi-simples (Colloque de Bruxelles, 1962)

Progrès dans le cas semi-simple :

Steinberg 1965 corps (parfait) de dim. coh. 1

$H^1(K, U) = 0$ si U semi-simple connexe

Chernosov 1989

$H^1(K, E_8) = 0$ K corps de nombres totalement imaginaire

Kneser, Harder

$H^1(K, U) = 0$ U semi-simple

Références

LNS

Cohomologie non abélienne:

M. Kneser, Tata Institute

(Jacobson : coh. gal. déguisée)

I. Satake

Cohomologie abélienne

G. Poitou, Coh. gal. des modules finis
Dunod, 1967

S. Shatz, Profinite groups, ...
Princeton, 1972

K. Haberland, Galois cohomology of number fields (Berlin 1978)

J. Milne, Etale Cohomology (1980)

J. Milne, Duality theorems (~1986)

H. Koch

Platonov, Principe de Hasse (à paraître).

Etude du $H^1(K,$ groupe semi-simple)

K quelconque ??

Cas orthogonal :
progrès grâce à Pfister, Merkurjev-Suslin, Arason, Rost, Jacob, ...

Groupes exceptionnels ?

Questions : $G_1 \longrightarrow G_2$

Est-ce que $H^1(K, G_1) \to H^1(K, G_2)$ injectif ?

Exemple : $G_2 \hookrightarrow SO_7$

$O(n) \longrightarrow O(3n)$

$x \longmapsto \begin{pmatrix} x & & \\ & x & \\ & & x \end{pmatrix} = x \otimes 1_3$.

Injectif (Pfister)

Démonstration par systèmes de racines ??

K'
| finie
K

$H^1(K, G) \to H^1(K', G)$
$\qquad\qquad\qquad \parallel$
$H^1(K, R_K^{K'} G)$

est-ce que c'est injectif ?

Springer : $[K' : K]$ impair, cas orthogonal $\Rightarrow$ injectivité
~ 1950

B-Lenstra : Même énoncé pour groupes unitaires

E_6, E_7, E_8

Exemples de corps sur lesquels on aimerait une réponse à ces questions

$K_0 = \mathbb{C}$, $K_1 = \mathbb{C}((T_1))$ séries formelles

$G_{K_1} \cong \hat{\mathbb{Z}} = \varprojlim (\mathbb{Z}/n\mathbb{Z})$ ($\hat{\mathbb{Z}}(1)$) canoniquement

$K_2 = K_1((T_2))$

$G_{K_2} = \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$

- - -

$G_{K_n} = \hat{\mathbb{Z}} \times \cdots \times \hat{\mathbb{Z}}$

Cohomologie de G_{K_n} dans un module fini = celle de $\mathbb{Z}^n$ (= celle du tore $\mathbb{T}^n$

$H^*(G_{K_n}, \mathbb{Z}/p\mathbb{Z})$ = algèbre extérieure sur $x_1, \ldots, x_n$ à coeff. dans $\mathbb{Z}/p\mathbb{Z}$

H^1 a comme base $x_1, \ldots, x_n$ dim n

H^2 $x_1 \wedge x_2, \ldots$ dim $\binom{n}{2}$

Problème:

$H^1(K_n, G_2) = ?$

F_4, E_6, E_7, E_8 ?

K quelconque (car $\neq 2$)

$H^1(K, G_2) \cong$ éléments décomposables de $H^3(K, \mathbb{Z}/2\mathbb{Z})$

décomposable : $x_1 x_2 x_3$, $x_i \in H^1(K, \mathbb{Z}/2\mathbb{Z})$

(cup produit)

élé de $H^1(K, G_2) \longleftrightarrow$ alg. d'octonions

$\longleftrightarrow$ 3-formes de Pfister

$\longleftrightarrow$ éléments décomposables.

H^3 a comme base $x_1 \wedge x_2 \wedge x_3 \cdots$

$H^1(K_n, G_2)$ = élé neutre

s/espaces de dim 3 d'un espace vect / $\mathbb{F}_2$ de dim n.

pts rationels / $\mathbb{F}_2$ de la Grassmannienne des 2-plans (projectifs) dans $\mathbb{P}_{n-1}$.

LN 5 : ces H^1 sont finis.

$H^1(K_n, F_4)$: connu ? Tits.

<u>Rappels</u> :

$$\begin{array}{l} L \\ \mid G \\ K \end{array}$$ galoisienne

"objets" X sur K

espace vectoriel muni de tenseurs d'un type donné (ex. forme quadratique) groupe algébrique

X_0 fixé

X tel que $X_L \cong X_{0L}$

<u>classes</u> de tels $X \Longleftrightarrow H^1(G, \mathrm{Aut}_L X_0)$

On choisit un isom.

$$X_{0L} \xrightarrow{\varphi} X_L$$

$s \in G$ $\quad s\varphi : X_{0L} \xrightarrow{\sim} X_L$

On peut donc définir $a_s \in \mathrm{Aut}_L X_0$

$a_s = \varphi^{-1} \circ s\varphi$

a_s est un cocycle : $a_{st} = \varphi^{-1} \circ st\varphi =$

$= \varphi^{-1} s(\varphi \circ a_t) = a_s \, {}^s a_t$.

φ modifié par un automorphisme de X_{0L} remplace a_s par un cocycle cohomologue

Injectivité : facile

Surjectivité : pas tjs vrai, il faut supposer quasi-proj. pour var. alg.

descente de Weil.

Classes d'objets sur K qui sont K_s-isom. à X_0

$$= H^1(K, \mathrm{Aut}\, X_0).$$

Exemples :

Formes quadratiques non dégénérées (car $\neq 2$)

$$x_1^2 + \cdots + x_n^2$$

$$x_1 x_2 + \cdots + x_{n-1} x_n \qquad (n \text{ pair})$$

classes de formes quadratiques $/K$ non dégénérées de rang n

$$\| $$

$$H^1(K, O_n).$$

carac 2

e.g. $x_1^2 + x_2 x_3$

l'énoncé devient faux : il faut prendre la cohomologie f.p.p.f (fidèlement plate

O_n pas lisse en car 2 (n impair)

$n = 1 \qquad x^2 = 1 \qquad O(1) = \mu_2$

pas lisse en carac. 2 (1 pt avec nilpotents)

$$H^1_{fppf}(K, \mu_2) = K^*/K^{*2}$$

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{G}_m \longrightarrow \mathbb{G}_m \longrightarrow 1$$

$$K^* \xrightarrow{2} K^{*2} \longrightarrow H^1(\mu_2) \to 0$$

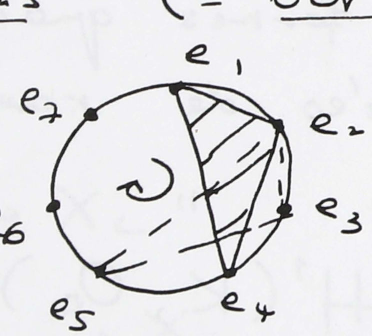
O_n n impair

$\det : O_n \longrightarrow \mu_2$, $SO_n = \mathrm{Ker}(\det)$

SO_n est lisse.

<u>classes d'octonions</u> (= <u>oct. de Cayley</u>)

(car $\neq 2$)



$e_0 = 1$

Oct. base $e_0, e_1, \dots e_7$

$e_1^2 = -1$, $e_2^2 = -1$, $e_4^2 = -1$ $e_1 e_2 = -e_2 e_1 = e_4$

$e_2 e_4 = -e_4 e_2 = e_1$, $e_4 e_1 = -e_1 e_4 = e_2$.

Mêmes règles pour tous les triangles.

"quaternions" sur e_i, e_{i+1}, e_{i+3}

$i \bmod 7$.

<u>Tous</u> les octonions : $e_1^2 = \alpha$, $e_2^2 = \beta$, $e_3^2 = \gamma$

$\alpha, \beta, \gamma \neq 0$.

$e_4 = e_1 e_2$, $e_4^2 = e_1 e_2 e_1 e_2 = -e_1 e_1 e_2 e_2 = -\alpha\beta$, etc.

classes d'octonions $= H^1(K, G_2)$

Algèbres de Lie simples de type G_2 sur K

Algèbres centrales simples de rang n^2
deviennent isom. à M_n sur K_s.

classes de telles algèbres $\longleftrightarrow H^1(K, \mathrm{Aut}\, M_n)$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \| $
$H^1(K, PGL_n)$.

$Br(K;n)$: s/gr de $Br(K)$ défini
par les alg. de rang n^2

$Br(K;n) \simeq H^1(K, PGL_n)$

$Br(K) \cong \varinjlim_n H^1(K, PGL_n)$

(rel. div.)

Descente générale de Grothendieck
Topologie étale
Base : "1 point" Spec K.

$H^1(K, PGL_n)$

$$1 \to \mathbb{G}_m \to GL_n \to PGL_n \to 1$$

$$H^1(K, PGL_n) \xrightarrow{\Delta} H^2(K, \mathbb{G}_m)$$

a_s : 1-cocycle PGL_n

b_s : relèvement dans GL_n

$c_{st} = b_s \, {}^s b_t \, b_{st}^{-1} \longrightarrow 1$ ds PGL_n

2-cocycle classe de $c_{st} = \Delta(\alpha)$

α classe de a.

On obtient ainsi

$$Br(K) \longrightarrow H^2(K, \mathbb{G}_m)$$

<u>Thm</u> c'est un isomorphisme.

<u>Produits croisés</u>

L gal. finie, $\gamma \in H^2(G, L^*)$

$|G$

K

$$1 \to L^* \to E_\gamma \xrightarrow{\pi} G \to 1$$

chaque fibre $\pi^{-1}(s) = E_s$ est un espace principal homogène (torseur) sous L^*.

$\tilde{E}_s = \{0\} \cup E_s$. On pose $\tilde{E} = \bigoplus \tilde{E}_s$.

$E_\gamma \subset \tilde{E}$

produit dans E_γ se prolonge K-linéairement en une structure d'algèbre sur $\tilde{E}_\gamma$.

Algèbre centrale simple, assoc. γ

On le vérifie pour $\gamma = 1$ (alg. de matrices)

cocycle se tue après ext. à L

$\rightarrow$ vrai en général.

$$Br(K) \xleftarrow{\sim} H^2(K, \mathbb{G}_m).$$

id. usuelle

(produits croisés)

On a vu précédemment

$$Br(K) \xrightarrow{\Delta} H^2(K, \mathbb{G}_m)$$

CG : les deux identifications diffèrent

CL ! par un signe.

3ème définition : Milne

Giraud

Grothendieck utilise l'identification par Δ.

1er Chapitre : Rappels sur les formes quadratiques

car$(K) \neq 2$.

Liés à $H^i(K, \mathbb{Z}/2\mathbb{Z}) = H^i(G_K, \mathbb{Z}/2\mathbb{Z})$

Notation $= H^i(K)$.

$\underline{H^1}$: suite exacte de Kummer

$$1 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 1 \qquad \text{car } K \nmid n$$

$H^1(K, \mathbb{G}_m) = 0$, donc on trouve

$$K^* \xrightarrow{n} K^* \to H^1(K, \mu_n) \to 0$$

$$H^1(K, \mu_n) \cong K^*/K^{*n} \qquad \text{"th. de Kummer"}$$

$n = 2$:
$$H^1(K) = K^*/K^{*2}$$
$$(a) \longleftarrow a \in K^*$$

Notation additive
$$(ab) = (a) + (b)$$

$$(a) = 0 \iff a \text{ est un carré dans } K$$

$$0 \to H^2(K, \mu_n) \to Br(K) \xrightarrow{n} Br(K)$$

d'où $H^2(K, \mu_n) \cong Br_n(K)$ si car.$K \nmid n$.

On choisit l'identification "produit croisé".

$$H^2(K, \mathbb{Z}/2\mathbb{Z}) \simeq Br_2(K).$$

Cup-produit :

$$H^i_A \times H^j_B \longrightarrow H^{i+j}_C \quad \text{si} \quad A \otimes B \to C.$$

au niveau des cocycles, facile à écrire

$f \quad g$

$$(f \cup g)(s_1, \dots, s_i, s_{i+1}, \dots, s_{i+j}) =$$

$$= f(s_1, \dots, s_i) \cdot {}^{s_1 \cdots s_i} g(s_{i+1}, \dots, s_{i+j}).$$

Cup-produit $H^1 \times H^1 \to H^2$ (mod 2) :

$$K^*/K^{*2} \times K^*/K^{*2} \longrightarrow Br_2(K)$$

Calcul montre que

$a \in K^*$, $b \in K^*$ $\longrightarrow$ $(a) \cup (b)$ = classe de l'alg. quat (a, b)

 $\overset{\shortparallel}{(a)(b)}$ $\qquad i^2 = a, j^2 = b$

calcul. Plus intéressant de le faire pour n quelconque :

$$\mu_n \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mu_n$$

$$H^1(K, \mu_n) \times H^1(K, \mathbb{Z}/n\mathbb{Z}) \longrightarrow Br_n(K)$$

$$\underbrace{K^*/K^{*2}}_{\substack{\Psi \\ b}} \times \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})$$
$$\qquad\qquad\qquad\qquad \Psi\ \chi$$

$b \in K^*$, $\quad \chi : G_K \to \mathbb{Z}/n\mathbb{Z}$

construire algèbre centrale simple

$(b)\cdot(\chi) \in \mathrm{Br}_n(K)$.

On peut se ramener au cas où χ est surjectif. χ définit une extension L/K cyclique de degré n, avec générateur choisi du groupe de Galois.

$H^2(G_{L/K},\ ) =$ pts fixes/normes

$$H^2(G_{L/K}, L^*) = \underset{\substack{\uparrow \\ b}}{K^*}/NL^*$$; d'où $[b] \in H^2(G_{\bar{K}/K}, \bar{K}^*)$ $\overset{\shortparallel}{\mathrm{Br}(K)}$.

On a : $(b)\cdot(\chi) = -\,\mathrm{cl}([b])$

Signe −

Correction à l'historique :

. Il faut parler de Kneser et Harder pour la nullité de $H^1 | K$ totalt imag s. connexe ($\neq E_8$)

. Cas des variétés abéliennes (et c. ell.)

. $\left.\begin{array}{l} {}^s\rho = A_s \rho A_s^{-1} \\ c_{s,t} A_{st} = A_s \, {}^s A_t \end{array}\right\}$ ne marche pas

${}^s\rho = A_s^{-1} \rho A_s$ oui !

Autres corrections

$L|K$ cyclique d'ordre n

$\mathrm{Gal}(L|K) = \mathbb{Z}/n\mathbb{Z}$

$b \in K^*$

$[b] \in H^2(L|K, L^*) \hookrightarrow Br_n(K) = H^2(K,$

$\chi : G_K \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$b \in K^* \longrightarrow (b) \in K^*/K^{*n} = H^1(K, \mu_n)$

$[b]_\chi \overset{?}{=} \pm (b) . \chi$ ds $H^2(K, \mu_n)$

$H^1(K, \mu_n) \times H^1(K, \mathbb{Z}/n\mathbb{Z})$

Signe correct : $-$

Preuve :

$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$

$\delta : H^1(K, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^2(K, \mathbb{Z})$

$\delta_\chi \in H^2(K, \mathbb{Z})$

$b \in H^0(K, \mathbb{G}_m)$

$b . \delta_\chi = \delta_\chi . b \in H^2(K, \mathbb{G}_m) = Br(K)$

$d^0 2 \quad 0$. (les 2 classes commutent)

On a :

$$[b]_\chi = \delta_\chi \cdot b$$

Lemme : $0 \to M_n \to M \xrightarrow{n} M \to 0$, M G-module (ici $M = \overline{K}^*$)

On se donne

$\chi \in H^1(G, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$

$m \in H^0(G, M)$

$\delta\chi \cdot m \in H^2(G, M)$ $\quad \delta\chi \in H^2(G, \mathbb{Z})$ $\quad \delta m \in H^1(G, M_n)$

$\chi \cdot \delta m = -\delta m \cdot \chi \quad \in H^2(G, M_n)$.

$i(\chi \cdot \delta m) \in H^2(G, M)$

On a $\quad i(\chi \cdot \delta m) = \delta\chi \cdot m \quad$ dans $H^2(G, M)$

$$\overset{\shortparallel}{(-i(\delta_m \cdot \chi)}$$

le résultat souhaité s'en déduit

Preuve du lemme On relève χ en $F : G \to \mathbb{Z}$

$\delta\chi$ est représenté par le cocycle

$$s, t \longmapsto \frac{F(s) + F(t) - F(st)}{n} \in \mathbb{Z}$$

$\delta m \quad$ On choisit $x \in M$ avec $nx = m$

$$s \longmapsto {}^s x - x \in M_n$$

$\delta\chi \cdot m$ est représenté par : $s, t \longmapsto (F(s) + F(t) - F(st$

$\delta m \cdot \chi$ $\quad$ ———— $\quad s, t \mapsto ({}^s x - x)\chi(t)$

$$\shortparallel$$

$$F(t)\, {}^s x - F(t)\, x$$

($\triangle$ χ à valeurs ds $\mathbb{Z}/n\mathbb{Z}$, pour distribuer la parenthèse, il faut utiliser F).

On ajoute : $F(s)x + F(t)^s x - F(st)x = \delta(f)(s,t)$

où $f(s) = F(s)x$

(Ou encore : règle de Leibniz !)

Cohomologie mod 2 de K ($car \neq 2$)

$H^1 = H^1(K) = \mathrm{Hom}(G_K, \mathbb{Z}/2\mathbb{Z}) = K^*/K^{*2}$

$a \in K^* \mapsto (a) \in H^1(K)$

$(a)(b) \in H^2(K) = Br_2(K)$

$(a)(b)$ représent. par l'alg. de quaternions

(a,b) $i^2 = a$, $j^2 = b$, $ij = -ji$

C Courbe de genre 0 (projective, lisse, absol. irréd, ...)

On peut lui associer $\mathrm{inv}(C) \in Br_2(K) \supset H^1(K, PGl_2)$

C devient isomorphe à P_1 sur K_s $\qquad Br(K,2)$

C décrit par un élément de $H^1(K, PGl_2)$

Conique associée à (a,b) $aX^2 + bY^2 - abZ^2 = 0$.

D alg. de quaternions (a,b)

$$\begin{cases} Trd = 0 \\ Nrd = 0. \end{cases} \quad \begin{cases} Xi + Yj + Zij = 0. \\ -aX^2 - bY^2 + abZ^2 = 0. \end{cases}$$

Autre interprétation

équat minimale $x^2 - Trd(x)x + Nrd(x) = 0$.

$C(D)$: cône des élts de D de $\square$ nul.

F : alg. de quaternions $\xrightarrow{\text{isom.}}$ conique

$\qquad\qquad Q \longrightarrow C_2$

$/_k$ commute aux ext. de scalaires

α 1-cocycle ds Aut D, $D \in C_1$

$$F({}_\alpha D) = {}_\alpha F(D) \quad \text{(cf LN 5)}.$$

Δ par torsion à partir de $D = M_2$

$F(\Delta) = {}_\alpha F(D)$ $\qquad F(D) = \mathbb{P}_1$

car $x \in M_2$ $x \neq 0$. , d'où $F(\Delta)$ est un $\mathbb{P}_1$ tordu.

$\mathrm{Im}\, x = L$ droite

$(\subset \mathbb{P}_1)$

Soit C de genre 0, construire D à partir de C ?

Intrinsequement (pour chx coord, cf + lr)

On fabrique un fibré E vectoriel de rang 2 sur C

$D = \mathrm{End}_k(E)$.

Si la conique n'a pas de pts, E indécomposable

Si $\mathbb{P}_1$, E décomposable.

Construction de E :

$$\begin{array}{l} C \times C \\ \big\downarrow \pi = pr_1 \\ C \end{array} \qquad \Delta \text{ diagonale} \qquad \mathcal{O}_{C \times C}(\Delta) \text{ fibré de rg 1}$$

(fctions ayt au + un pôle simple sur Δ).

$\underline{E} = \pi_* \mathcal{O}_{C \times C}(\Delta)$ $\qquad$ La fibre en P, E_p = fctions rationnelles sur C ayt au plus 1 pôle simple en P, est de dimension 2.

$(R^1\pi_* = 0)$

$$0 \longrightarrow \underset{\substack{\text{(fibré trivial} \\ \text{de rg 1)}}}{\underline{1}} \longrightarrow E \longrightarrow \underset{\text{fibé tgt}}{T} \longrightarrow 0$$

$H^1(C, \mathrm{Hom}(T,1)) = H^1(C, \Omega^1)$

Exercice : Comparer la classe definissant E comme extension à la classe fondamentale de la dualité.

(Prob^r ± 1, car sinon on aurait des ennuis dans la carect correspondante à ce nbre, ce qui n'est pas).

Si $C = \mathbb{P}$, $\quad E = \mathcal{O}(-1) \oplus \mathcal{O}(-1)$

$D = \mathrm{End}_K(E) = M_2$

$(a)(b) \in H^2(K)$

Formules évidentes

$(a)(-a) = 0 \qquad a \in K^*$

$(a, 1-a) = 0 \qquad a \neq 0, 1$

$(a)(b) = 0$ ssi l'éq $aX^2 + bY^2 - abZ^2 = 0$ (ou encore $Z^2 - aX^2 - bY^2 =$ a une solution $\neq (0,0,0)$ ds K $\Leftrightarrow$ b norme de l'ext. $K(\sqrt{a})|K$ $\Leftrightarrow$ a norme ds $K(\sqrt{b})|K$.

1e cas $\quad aX^2 - aY^2 + a^2Z^2 = 0 \quad X = 1, Y = 1, Z = 0.$

2e cas $\quad aX^2 + (1-a)Y^2 - a(1-a)Z^2 = 0$

ou encore $Z^2 - aX^2 - (1-a)Y^2 = 0. \quad X = Y = Z =$

Débouche sur la K-théorie de Milnor ...

On va détailler un peu $(a)(a) = (-1)(a)$.

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

$\delta : H^i(G, \mathbb{Z}/2\mathbb{Z}) \to H^{i+1}(G, \mathbb{Z}/2\mathbb{Z})$. opération de Bockstein (modulo p) $= Sq^1$ (puis. de Steenrod)

$\delta x = 0$.

<u>Formule</u> $\boxed{\delta x = x^2}$ si $i = 1$

Pour démontrer cela, on utilise exemple universel

$x \in H^i(X, A)$

X cplexe simpl. par ex.

i, A fixé

On veut prouver une formule pour $\forall x, X \ldots$

$X \xrightarrow{f_x} K(A, i)$ complexe d'Eilenberg MacLane

$\pi_i = A$ $\pi_j = 0$ $j \neq i$

$\iota \in H^i(K(A,i), A)$

Toute classe de cohom est obtenue à partir de ι : si formule vraie pour ι, vraie pour tout x.

Ici $S_N / \pm 1 = \mathbb{P}_N(\mathbb{R})$ S_N : sphère

$\pi_1 = \mathbb{Z}/2\mathbb{Z}$

$\pi_j = 0$ $j \neq 1$, $j < N$

"$N = \infty$" on a le $K(A, i)$.

La cohomol. est la cohom mod 2 de l'esp proj réel

$\dim H^i = 1$ et l'algèb. de cohom est une alg de de polynomes en $i \in H^1$

$1, i, i^2, i^3, \ldots$

$$\delta i = \begin{cases} 0 \\ i^2 \end{cases}$$ mais si 0, ce serait vrai toujours (impossi
Donc c'est i^2.

On peut rédiger le même argument en restant à l'intérieur de la théorie des groupes

$x \in H^1(G, \mathbb{Z}/2\mathbb{Z})$

C_2 gr. cycl. d'ordre 2

$G_2 \xrightarrow{f} C_2$

$x = f^*(i)$

En fait, même preuve car $BC_2 = K(\mathbb{Z}/2\mathbb{Z}, 1)$
$\shortparallel$
classifiant de C_2

Retour sur $\delta x = x^2 \quad x \in H^1(K)$

$\delta x = (-1)(x)$

(-1) classe de -1 ds K^*/K^{*2}, $= 0$ si $i \in K$, $\neq 0$ sinon

(-1) corresp à l'hom $G_K \to \mathbb{Z}/2\mathbb{Z}$ associé à l'ext. $K(i)$

Cor : Si car $K = p \qquad p \equiv 1 \pmod 4 \Rightarrow (-1) = 0$

$\delta x = 0$

Classes de cohomologie "négligeables"

G fini, M G-module

$x \in H^i(G, M)$

Déf. : x K-négligeable (K fixe) si pour tout homomorphisme : $G_K \xrightarrow{f} G$,

$$f^* x = 0 \quad \text{dans } H^i(K, M)$$

Déf. : x négligeable si x K-néglig. pour tout K.

En fait, il y a beaucoup de telles classes

$H^i_{\text{utile}}(G, M) = H^i / H^i_{\text{négl}}$ "petit".

Exemples : en cohom modulo 2

- G gpe fini, u et $v \in H^1(G) = H^1(G, \mathbb{Z}/2\mathbb{Z})$

Soit $x = uv(u+v) = u^2v + uv^2 \in H^3(G, \mathbb{Z}/2\mathbb{Z})$

Alors x est négligeable, car dans $H^3(K)$ on a $u^2v = (-1)uv = uv^2$.

si $G = (2, \dots, 2)$ $\quad H^*(G) =$ alg. de polyn eng. par n élts de degré 1.

Si u et v st 2 générat $\neq$, $x \neq 0$.

D'autre part, soient u_K, v_K, x_K les classes ds $H^1(K), H^1(K), H^3(K)$

car $K = 2 \implies H^1(K) = 0$ à partir de 2

car $K \neq 2 \implies u_K^2 = (-1)_K u_K$

$$x_K = (-1)_K u_K v_K + (-1) u_K v_K = 0.$$

Quelques remarques "négligeables"

- Dans le cas des 2-gpes, les classes nég st l'idéal engendré par (u^2v+uv^2)

- Si K car p, $p \equiv 1 \mod 4$ (si K contient i), $x \in H^1 \Rightarrow x^2 \in H^2$ est K-négligeable

- On verra que la cohomologie utile mod 2 s'arrête.

- Si $y \in H^2(G)$, δy est négligeable

H^3

On utilise Merkuriev-Suslin : Tout élt de $H^2(G_K)$ est somme de produits $u_i, v_i \in H^1(G_K)$.

Donc il suffit de prouver que $\delta(u.v) = 0$ si $u, v \in H^1(G_K)$.

$$\delta(u.v) = \delta u . v + u . \delta v = u^2 v + uv^2$$

<u>Une</u> <u>formule de cobord</u>.

Soit $0 \to A \to B \xrightarrow{\pi} C \to 0$.

suite exacte de G-modules

Soit χ_s 1-cocycle de G à valeurs ds $\mathrm{Hom}(C, A)$. On en déduit une nouvelle action de G sur B :

$${}^{s'}b = {}^{s}b + \chi_s({}^{s}\pi b).$$

Soit $B_\chi = B$ avec cette action.

Soient $\delta : H^i(G, C) \longrightarrow H^{i+1}(G, A)$

et

$\delta_\chi : H^i(G,C) \to H^{i+1}(G,A)$ les cobords correspondants.

<u>Formule</u> : $\delta_\chi(x) = \delta(x) + (\chi) \cdot x$

$x \in H^i(G,C) \qquad (\chi) \in H^1(G, \mathrm{Hom}(C,A))$

$C \times \mathrm{Hom}(C,A) \longrightarrow A.$

<u>Preuve</u> : $f = f(s_1, \dots, s_i)$ i-cochaîne ds B relevant un cocycle de C, f_c, de classe x

$\delta(x)$ représ. par $(s_1, \dots, s_{i+1}) \mapsto {}^{s_1}f(s_2, \dots, s_{i+1}) - f(s_1, s_2, \dots, \dots) + \dots$

$\delta_\chi \qquad \mapsto {}^{s_1'}f(\quad) - \dots$

$\delta_\chi(x) - \delta(x)$ repres par le cocycle

$s_1, \dots, s_{i+1} \longmapsto \chi_{s_1}({}^{s} f_c(s_2, \dots, s_{i+1}))$

$\qquad\qquad \shortparallel$ cup-produit

Applications (car $K \neq 2$)

$*$ $\delta x = (-1)\, x$

$0 \to \mu_2 \to \mu_4 \to \mu_2 \to 0 \qquad (*)$.

$\qquad \shortparallel \qquad\qquad \shortparallel$

$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$

On passe de l'une à l'autre par $\chi \in H^1(K, \mathbb{Z}/2\mathbb{Z})$

$\chi = (-1)$

$\delta_{(*)} : H^1(K,\mu_2) \to H^2(K,\mu_2)$

$\delta_{(*)}$ associé à $(*)$ est 0

$H^1(K,\mu_n) = K^*/K^{*n}$

$K^*/K^{*4} \to K^*/K^{*2} \xrightarrow{\delta} H^2($

surjective !

$0 = \delta_*(x) = \delta(x) + (x)(-1) \longrightarrow \delta(x) = (x)(-1)$.

* Soit p premier $\neq 2$, car $K \neq p$.

$H^i(K, \mathbb{Z}/p\mathbb{Z}) = H^i(K)$

$\delta : H^i(K) \to H^{i+1}(K)$

Bockstein $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$

δx ? $x \in H^1(K)$

$\varphi \in H^1(K)$ associé à μ_{p^2}

L'action de G_K sur μ_{p^2} définit $\varphi : G_K \to (\mathbb{Z}/p^2\mathbb{Z})^* \xrightarrow{\varepsilon} \mathbb{Z}/p\mathbb{Z}$

ε unique homomorphisme qui applique la classe modulo p^2 de $1+2p$ sur $2 \bmod p$.

$\iff$ n classe mod p^2 $(n,p)=1$.

$$\frac{n^{p-1}-1}{p} = -\varepsilon(n) \bmod p.$$

Formule : $\boxed{\delta x = x \cdot \varphi}$ $\quad x \in H^1(K)$, $\varphi \in H^1(K)$

2 preuves : Il suffit de prouver cette formule

quand K contient μ_p (car $K' = K(\mu_p)/K$ de d° 1er à p et donc $H^i(K, \;) \hookrightarrow H^i(K')$).

$$\varphi : G_K \longrightarrow \mathbb{Z}/p\mathbb{Z} = \{\text{élts} \equiv 1 \bmod p\} \pmod{p^2}$$

La suite $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$.

tordue, en choisissant z racine primitive p-ième de 1 ds K, donne

$$0 \to \mu_p \to \mu_{p^2} \to \mu_p \to 0.$$

μ_p "=" $\mathbb{Z}/p\mathbb{Z}$ via z $\qquad s \in G_K : \; s\zeta = \zeta^{1+\varepsilon(s)p} = \zeta \cdot z^{\varepsilon(s)}$

φ tord l'action de μ_p

$\zeta^p = z$.

Or le cobord de cette suite est 0, donc le cobord de la suite triviale est $\delta x = -(\varphi) \cdot x = x \cdot (\varphi)$

Autre preuve via algèbres cycliques ds $Br_p(K)$
(φ) = classe de (z).

<u>Corollaire</u> G fini $p \neq 2$

$u \in H^1(G)$

$u \cdot \delta(u) \in H^3(G)$

$u \cdot \delta(u) = \cancel{} = u \cup \varphi = 0.$

donc $u \cdot \delta(u)$ est négligeable

Idem pour $\delta(u)\,\delta(u) \in H^4(G)$

$G = C_p$ dim $H^i(G) = 1$ pour tout i, négligeable pour $i \geq 3$

H^0 1 $\quad H^2$ δu $\quad H^3$ $u \cdot \delta u$ $\quad H^4$ $\delta u\, \delta u$ ...

H^1 u

Compléments

i) Coh. "négligeable"

$x \in H^i(G,V)$ G fini

K $\quad G_K \xrightarrow{\varphi} G$ $\quad \varphi^* x = 0$

$G_K = \mathrm{Gal}(K_s/K)$

$$\begin{array}{c} Y \\ \downarrow G \\ X \end{array} \quad H^*(G) \to H^*(X) \qquad X \to BG$$

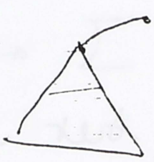
Analogue

cohom. négligeable pour la | top. étale $\Leftrightarrow x = 0$
| top. usuelle

BG = classifiant du gpe G, sa cohom est celle de G.

d'où le résultat pour la top. usuelle.

Pour "étale" X complexe simplicial fini



$\exists$ esp. alg. (affine) / $\mathbb{C}$ qui a le même type d'homotopie que X.

X: $(x_i)_{i \in I}$ $\quad x_i \in [0,1]$ $\quad \sum x_i = 1$

supp $(x_i) \subset$ complexe

On fabrique l'espace en supprimant les cond réelles

soit z_i, $z_i \in \mathbb{C}$, $\sum z_i = 1$, support $\subset$ comp

Ex X: •—• $\quad x_1, x_2$ $\quad x_1 + x_2 = 1$, $x_i \geq 0$

$X_{\mathbb{C}}$ $\quad$ plan complexe a un type d'hom.

En général, on écrit les rétractions et cela marche.
Malheureusement, bcp de singularités et il n'existe pas de manière de les supprimer en gardant le type d'hom.

On peut aussi imiter BG en se restreignant aux var alg / $\mathbb{C}$, lisses
cf var de Stiefel.

$\mathbb{C}^N = \mathrm{Aff}^N(\mathbb{C})$

$z_1, \dots, z_n$ $\quad z_i \in \mathbb{C}^N$ $\quad z_i$ lin. ind.

$V_{N,n}$ $\quad GL_n$ opère libr^t sur $V_{N,n}$

$G \subset GL_n$

G opère librement sur $V_{N,n}$

$V_{N,n}$ var. lisse connexe, à cohom. nulle jusqu'à $2N-(2n+1)$ (?)

$\downarrow$

$V_{N,n}/G$ $\quad \to \infty$ avec N.

$H^*(G) \to H^*(V_{N,n}/G)$ injectif jusqu'à cette dim.

N grand : pas de classes négligeables !

Mais : $\begin{array}{c} Y \\ \downarrow G \\ X \end{array}$ X négligeable

la classe de X se tue sur un ouvert de Zariski assez petit

$\boxed{2) \quad K \text{ car. } p > 0.}$

Décrire $Br_p K$?

Produits croisés cycliques

1° $a \in K$, $b \in K^*$ donnés

$[a, b) \in Br_p K$

a définit une extension de type Artin-Schreier $X^p - X = a$

et $y^p = b$ $\quad yxy^{-1} = x + 1$

$\begin{array}{c} K_a \\ \big| \, \mathbb{Z}/p\mathbb{Z} \\ K \end{array}$ $\quad [a, b) = 0 \iff b$ est une norme de K_a

$\xi \in Br_p K$ est de la forme $[a, b)$

a imposé $\iff \xi$ scindé (= annulé par K_a)

b imposé $\iff \xi$ annulé par $K(\sqrt[p]{b})$

(2) $a, b \in K$

$[a,b] \in Br_p K$

$x^p = a \quad y^p = b \quad xy - yx = 1.$

$[a,b] = [ab, b)$ si $b \neq 0$

$= 0$ si $b = 0.$

$\Omega^1 K$ 1-formes $\sum a_i db_i$

avec $a(a_i db_i) = (aa_i) db_i$

$d(bc) = bdc + cdb$

$\Omega^1 K \longrightarrow Br_p K$

$\sum a_i db_i \longmapsto \sum [a_i, b_i] \in Br_p K.$

$\sum a_i \dfrac{db_i}{b_i} \longmapsto \sum [a_i, b_i) \in Br_p K$

Albert, Witt, ...

c'est surjectif, les diff. exactes db donnent 0 ds Br_p.

$\Omega^1 K \xrightarrow{F-1} \Omega^1 K / dK \longrightarrow Br_p K \longrightarrow 0.$

$F\ \sum a_i \dfrac{db_i}{b_i} \longmapsto \sum a_i^p \dfrac{db_i}{b_i} \in \Omega^1 K / dK$

= "inverse de l'opérateur de Cartier".

cf Witt Hamb. Abhand. 1958

Pour $p = 2$

$[a,b] \longmapsto$ conique corresp.

$X^2 + aY^2 + bZ^2 + YZ = 0.$

$[a,b) \longrightarrow X^2 + bY^2 + abZ^2 + bYZ = 0$

3°)

C genre 0.

$0 \to 1 \to E \to T \to 0$.

$x \in H^1(\cancel{\ } C, \Omega^1)$ $= \pm$ classe f. de la dualité ?

La construction est tout à fait universelle

$x = n \in \mathbb{Z}$ $\quad \mathbb{P}, /\mathbb{Z}$.

p premier $\Rightarrow p \nmid n$

car sinon en car p, l'extension serait triviale

donc $n = \pm 1$

Formes quadratiques et leurs invariants cohomologiques

car $K \neq 2$.

K_s, $G_K = Gal(K_s/K)$ $\quad H^i(G_K) = H^i(K) = H^i(G_K, \mathbb{Z}/2\mathbb{Z})$

Un des buts est d'associer aux formes des invariants qui les caractériseraient.

- langage e.v V de dim finie, muni d'une forme q quad. (non dég.) (à isom. près)
- langage $f(x_1, \dots, x_n) = \sum a_{ij} x_i x_j$ $\quad a_{ij} = a_{ji}$ $\quad a_{ij} \in K$ $\quad d = \det(a_{ij}) \neq 0$

$f \sim f'$ s'il existe une transf. inversible des x_i amenant f sur f'.
$(a'_{ij}) = {}^tC . (a_{ij}) C$ avec $C \in Gl_n$

$f \sim \sum a_i x_i^2$ $\quad a_i \in K^*$
$\Updownarrow$
V a une base orthogonale (e_i)

$\left| \begin{array}{l} x.x = q(x) \\ x\, y = \frac{1}{2}(q(x+y) - q(x) - q(y)) \end{array} \right.$

$e_i e_j = 0$ $i \neq j$.

$a_i \in K^*$ $\quad q(x) = \sum a_i x_i^2$ $\quad q = \langle a_1, \dots, a_n \rangle$

$\langle a_1, \dots, a_n \rangle \overset{?}{\simeq} \langle b_1, \dots, b_n \rangle$

Les formes à deux variables décident de cette question

$n \geq 2$ $\quad \{a_1, \dots, a_n\}$, $\{b_1, \dots, b_n\}$ sont 2-voisines si $a_i = b_i$ pour tout i sauf au plus 2 valeurs et $\langle a_j, a_k \rangle \simeq \langle b_j, b_k \rangle$.

Thme (Witt) Si $\langle a_1, \dots, a_n \rangle \simeq \langle b_1, \dots, b_n \rangle$, il existe une chaîne (finie) de formes 2-voisines de la précédente allt de $\langle a_1, \dots, a_n \rangle$ à $\langle b_1, \dots, b_n \rangle$.

ie le graphe des $\langle b_1, \dots, b_n \rangle \simeq \langle a_1, \dots, a_n \rangle$ est connexe (arête existe si formes 2-voisines)

$V, q \quad n \geq 3$

$\mathcal{E} = (e_1, \ldots, e_n)$ base orthog. de V

$\mathcal{E}$ voisine de $\mathcal{E}'$ si $e'_i = e_i$ pour au moins un i

Thme le graphe des bases orthogonales est connexe

"Générateurs : formes à 1 variables

Relations " formes à 2 variables".

Ce principe va permettre de définir des invariants

Inv. coho m : <u>classes de Stiefel-Whitney</u>.

(cf Delzant, fin des années 50).

$q = \langle \alpha_1, \ldots, \alpha_n \rangle$

$\downarrow$

$w_i(q) \in H^i(K)$.

$\bigoplus_{i \geq 0} H^i(K) = H(K)$

$w(q) = 1 + w_1(q) + w_2(q) + \ldots \quad \in H(K)$

$w(q) = \prod (1 + (\alpha_i))$

$\alpha \in K^* \longmapsto (\alpha) \in H^1(K) = K^*/K^{*2}$ écrit additivement

$w_1(q) = \Sigma(\alpha_i) = (\alpha_1 \ldots \alpha_n) = (d)$

$w_2(q) = \sum_{i<j} (\alpha_i)(\alpha_j)$.

$w_i(q) =$ i-ème fction symétrique élémentaire des (α_i)

<u>Prop.</u> (Delzant) <u>Si</u> $\langle \alpha_1, \ldots, \alpha_n \rangle \cong \langle \beta_1, \ldots, \beta_n \rangle$, <u>alors</u> $\prod (1 + (\alpha_i)) = \prod (1 + (\beta_i))$ <u>dans</u> $H(K)$.

On est ramené au cas $n = 2$

$\alpha_1 X^2 + \alpha_2 Y^2 \simeq \beta_1 X^2 + \beta_2 Y^2 \overset{?}{\Rightarrow} (\alpha_1 \alpha_2) = (\beta_1 \beta_2)$ disc.

$(\alpha_1)(\alpha_2) = (\beta_1)(\beta_2)$ dans $H^2(K$

V, q e.v. quad.
alg. de Clifford $C(V)$
eng. par V $\quad x \in V \quad x \cdot x = q(x)$
$C(V) =$ alg. de quat. (α_1, α_2) $\quad e_1^2 = \alpha_1 \quad e_2^2 = \alpha_2 \quad e_1 e_2 = -e_2 e_1$
idem sur β d'où l'égalité.

$q = \langle \alpha_1, \dots, \alpha_n \rangle$
$w_n(q) = \pi(\alpha_i) \in H^n(K)$.
$w_2(q) =$ "invariant de Hasse-Witt".
$w_3 = w_1 w_2 \qquad \sum(\alpha_i) \sum_{j<k} (\alpha_j)(\alpha_k) = 3 w_3 + \sum_{j<k} \big((\alpha_j)(\alpha_j)(\alpha_k)$
$+ (\alpha_j)(\alpha_k)(\alpha_k)\big)$

- 3 mod 2, c'est 1 !
- le reste est négligeable $\big((\alpha_j)^2(\alpha_k) + (\alpha_j)(\alpha_k)^2\big)$
$0 = (-1)(\alpha_j)(\alpha_k) + (\alpha_j)(-1)(\alpha_k)$

cf Milnor (Invent. Math.) Si i n'est pas une puissance de 2, w_i peut s'écrire comme polynôme en les w_j, $j < i$. Plus précisément :
Si l'on écrit $i = 2^{r_1} + 2^{r_2} + \dots + 2^{r_k}$, $r_1 < \dots < r_k$,
on a : $w_i = w_{2^{r_1}} \dots w_{2^{r_k}}$.

<u>Autre</u> <u>invariant</u> (n pair ≥ 4)
① $(d) = (1) = 0$
$q = \langle \alpha_1, \dots, \alpha_n \rangle \qquad u(q) = (\alpha_1) \dots (\alpha_{n-1}) \in H^{n-1}(K)$
<u>Proposition</u> : $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$
$\Rightarrow (\alpha_1) \dots (\alpha_{n-1}) = (\beta_1) \dots (\beta_{n-1}) \in H^{n-1}(K)$

Ne dépend en fait pas de l'indice qu'on laisse tomber

$$(\alpha_2)(\alpha_3)\cdots(\alpha_n) \overset{?}{=} (\alpha_1)(\alpha_2)\cdots(\alpha_{n-1})$$

$$(\alpha_n) = (\alpha_1) + \cdots + (\alpha_{n-1})$$

$$(\alpha_2)(\alpha_3)\cdots(\alpha_{n-1}) \sum_{i=1}^{n-1} (\alpha_i) = (\alpha_1)(\alpha_2)\cdots(\alpha_{n-1}) + \sum_{i=2}^{n-1} (\alpha_2)(\alpha_3)\cdots(\alpha_i)^2(\alpha_{i+1})\cdots(\alpha_{n-1})$$

$$= (\alpha_1)(\alpha_2)\cdots(\alpha_{n-1}) + \{ \underset{\text{pair}}{n-2} \text{ fois un terme}$$

Par le lemme de Witt, il suffit de vérifier que si $\beta_3 = \alpha_3, \ldots, \alpha_n = \beta_n$ et $\langle \alpha_1, \alpha_2 \rangle \simeq \langle \beta_1, \beta_2 \rangle$, on a la formule voulue.

$$(\alpha_1)(\alpha_2)(\alpha_3)\cdots(\alpha_{n-1}) = (\beta_1)(\beta_2)(\alpha_3)\cdots(\alpha_{n-1}) \in H^{n-1}(K)$$

Soit $i(q) = (\alpha_1)\cdots(\alpha_{n-1}) \in H^{n-1}(K)$.

② Cas général

d disc. $(d) = w_1$

invariant $i(q) \in H^{n-1}(K)/w_1 H^{n-2}(K)$

image de $(\alpha_1)\cdots(\alpha_{n-1})$.

$K_d = K(\sqrt{d})$ d non carré

$(\alpha_1)_{K_d} \cdots (\alpha_{n-1})_{K_d} \in H^{n-1}(K_d)$ est un invariant de la forme quadratique

$K_d = K(\sqrt{d})$ **Prop.** $H^i(K) \xrightarrow{\text{Res}} H^i(K_d) \xrightarrow{\text{Cor.}} H^i(K) \to H^{i+1}(K)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad x \mapsto d x$

$\quad |$
$\quad K$

suite exacte

$H^i(K)/dH^{i-1}(K) \hookrightarrow H^i(K_d)$

Suite exacte des extensions quadratiques

Analogue en topol. usuelle fibration par S_n, $n=0$

Soit G un groupe ~~discret~~ | ou discret profini et H un ss gpe d'indice 2 de G ; soit $\varepsilon : G \to \{\pm 1\}$ le caractère de noyau H.

A G-module

A_ε module A "tordu par ε". On a la suite exacte :

$A \otimes \mathbb{Z}_\varepsilon$

$$H^i(G, A_\varepsilon) \xrightarrow{Res} H^i(H, A) \xrightarrow{Cor} H^i(G, A) \xrightarrow{\delta} H^{i+1}(G, A_\varepsilon$$

$$\delta x = a_\varepsilon x$$

où $a_\varepsilon \in H^1(G, \mathbb{Z}_\varepsilon) = \mathbb{Z}/2\mathbb{Z}$

représenté par le cocycle $s \mapsto \begin{cases} 0 & \text{si } s \in H \\ 1 & \text{si } s \notin H. \end{cases}$

Rque $\quad G \to G/H \underset{C_2}{\overset{\|}{}}$ $\quad H^1(G/H, \mathbb{Z}_\varepsilon) = \mathbb{Z}/2\mathbb{Z} \hookrightarrow H^1(G, \mathbb{Z}$

si G profini, c'est un isomorph

Si $A = \mathbb{Z}/2\mathbb{Z}$, A_ε c'est A !

$$H^i(G) \to H^i(H) \to H^i(G) \to H^{i+1}(G) \to$$

A^* : module induit $\mathrm{Ind}_H^G A = A \otimes \mathbb{Z}[G/H]$

$$0 \to A_\varepsilon \to A^* \to A \to 0$$

$$0 \to \mathbb{Z}_\varepsilon \to \mathbb{Z}[G/H] \to \mathbb{Z} \to 0$$

$$e_1 - e_2 \qquad e_1, e_2 \mapsto 1$$

$$0 \to A_\varepsilon \to A \oplus A_\varepsilon \to A \to 0.$$

mais l'action de groupe est une action tordue !

On a vu une formule générale la dernière fois pour les "tordues" → cup produit, ici $a_\varepsilon \cdot x$.

Thme (Witt) Les formes de ~~degré~~ $n \leq 3$ sont classées par w_1, w_2.
dimension
rg

Thme (Arason, ...) Les formes de ~~degré~~ 4 à discriminant carré st classées par w_1, w_2 et $i \in H^3(k)$.
dimension
rg

$n = 1$ $\quad w_1$

$n = 2$ $\quad q_3^\# = \langle 1 \rangle \oplus q \quad n_3^\# = 3$

inv. identiques pr q et q_3

Par le thme de simpl. de Witt $\quad q_3 \sim q'_3 \Rightarrow q \sim q'$
(cf prochaine fois)

on est ramené au cas:

$n = 3$ $\quad q, q'$ $\quad$ m w_1, w_2

d discrim.

dq et dq' ont disc. 1.

On a des formules donnant $w_i(\lambda q)$ en termes de (λ) et de $w_i(q)$.

$$q = \langle \alpha, \beta, \gamma \rangle \qquad \lambda \in k^* \qquad \lambda q = \langle \lambda\alpha, \lambda\beta, \lambda\gamma \rangle$$

$$w_2(\lambda q) = (\lambda\alpha)(\lambda\beta) + (\lambda\alpha)(\lambda\gamma) + (\lambda\beta)(\lambda\gamma).$$

$$= ((\lambda) + (\alpha))((\lambda) + (\beta)) + \cdots$$

$$w_2(\lambda q) = (\lambda)(\lambda) + w_2(q)$$

$$= + (-1)(\lambda) + w_2(q).$$

On peut donc supposer que $d(q) = 1$.

la forme $q = \langle \alpha, \beta, \alpha\beta \rangle$

$-q \simeq -\alpha X^2 - \beta Y^2 + \alpha\beta Z^2$ = Norme (alg. de quat (α, β)) sur les élts de trace 0.

$$w_2(q) = (\alpha)(\beta) + (\alpha)(-\alpha\beta) + (\beta)(-\alpha\beta)$$

$$= \underset{\binom{\shortparallel}{1}}{3}(\alpha)(\beta) + (\alpha)(\alpha) + (\beta)(\beta) + (-1)(\alpha) + (-1)(\beta)$$

$$= (\alpha)(\beta) + \cancel{(-1,\alpha\beta)}.$$

$$w_2(q) = (\alpha)(\beta).$$

Remarque : On considère ici comme forme triviale les sommes de carrés, d'inv. nul.
Mais la forme naturelle en rg pair serait plutôt la forme hyperbolique. On verra les formules correspondantes la prochaine fois.

$n=4$ $\quad q = \langle\alpha_1\rangle \otimes \underbrace{(\langle 1\rangle + \langle\lambda\rangle + \langle\mu\rangle + \langle\lambda\mu\rangle)}_{\shortparallel}$

Norme d'une alg. de quaternion $(-\lambda, -\mu)$

Pour connaître q, il faut connaître cette alg D et aussi $\alpha_1 \in K^*/ND^*$

En fait $K^*/ND^* \subset H^3(K)$ et α_1 envoyé là-dedans est justement $i(q)$.

W_2 détermine D

i —— classe de α_1 modulo les normes réduites

$$K^*/ND^* \longrightarrow H^3(K)$$
$$x \in K^* \longmapsto (x).[D] \quad \text{cf prochaine fois.}$$

28/1/91

K car $\neq 2$.

$q \quad w_i(q) \in H^i(K) = H^i(G_K, \mathbb{Z}/2\mathbb{Z})$.

rang $q \leq 3 \quad$ w_1, w_2 classifiant

rang $q = 4 \quad$ dis $\square$ $(w_1 = 0) \quad w_2$ et $i(q) \in H^3(K)$ classifiant

q

dis non $\square$?

$\langle a_1, \dots, a_4 \rangle = \langle a_1 \rangle \oplus \dots \oplus \langle a_4 \rangle \qquad a_1 \dots a_4 = \square$

$q = \langle a_1 \rangle \otimes (\langle 1 \rangle \oplus \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \langle b_1 b_2 \rangle) \qquad a_2 = a_1 b_1$

$\downarrow \qquad a_3 = a_1 b_2$

forme norme de l'algèbre de quaternions $(-b_1, -b_2) = D_q$

$$w_2(q) = (b_1)(b_2) + (b_1)(b_1 b_2) + (b_2)(b_1 b_2)$$
$$= (b_1)(b_2) + (-1, b_1 b_2)$$
$$= (-b_1)(-b_2) + (-1)(-1)$$

$[D_q] \in H^2(K)$
$\shortparallel$
$w_2(q) + (-1)(-1)$

$q \begin{cases} D \text{ alg. de quat} \\ \underline{a} \in K^*/ND^* \end{cases}$

Thme: <u>Mercurief</u> <u>Suslin</u> $\quad K^*/ND^* \longrightarrow H^3(K)$

$a \in K^* \longmapsto (a) \cdot [D]$

(on trouve 0 si a est une norme)

<u>Cet homomorphisme est injectif</u>

$$i(q) = (a_1)(a_1 b_1)(a_1 b_2) = (a_1)(-1)(-1) + (a_1)(-1)(b_1)$$
$$+ (a_1)(-1)(b_2) + (a_1)(b_1)(b_2)$$
$$= (a_1)[D_q].$$

C'est faux si le disc. n'est pas □.

$i(q) \in H^3(K)/(d)H^2(K) \subset H^3(K_d)$

$K_d = K(\sqrt{d})$

Remarque Supposons que $K \ni i$, de sorte que $(-1)=0$
Alors les formes q et dq ont les mêmes invariants w_1, w_2, i

$$w_2(\lambda q) = n_2(\lambda)(-1) + n_1(\lambda) w_1(q) + w_2(q)$$

$n_1 = n-1$ $\quad n_2 = \frac{n(n-1)}{2}$

$n=4$: $\equiv 1 \mod 2$ $\quad \equiv 0 \mod 2$

$$w_2(dq) = (d)(-d) + w_2(q) = w_2(q)$$

L'invariant i se calcule sur K_d où d est un carré donc $dq \sim q$ sur K_d.

Il suffit donc de trouver un ex où $dq \neq q$ sur K

$k = \mathbb{Q}(i)$ $\quad \alpha, \beta \in k^*$ $\quad (\alpha, \beta) \neq 0$.

ex: $\alpha = 2+i$ $\quad \beta = 3$

$\not{=}$ = corps de quaternions ramif. en $2+i$ et 3

$K = k(T)$ $\quad T$ indét.

$q = \langle 1, \alpha, \beta, T \rangle$ $\quad d = \alpha\beta T$

$dq = \langle \alpha\beta T, \beta T, \alpha T, \alpha\beta \rangle$

Par ex: q ne représente pas $\alpha\beta$

Ou bien: classif. des formes

$q \oplus (-dq)$ 8 variables

si les 2 formes isomorphes, ce serait hyperbolique

Or celle-ci est anisotrope car c'est

$\langle 1, \alpha, \beta, \alpha\beta, T, \alpha T, \beta T, \alpha\beta T \rangle$

$= \underbrace{\langle 1, \alpha, \beta, \alpha\beta \rangle}_{\text{anisotrope}} \oplus T \langle 1, \alpha, \beta, \alpha\beta \rangle$

car alg quot = corps.

$<1, \alpha, \beta, \alpha\beta>$ anisotrope car l'alg de quat (α, β) est un corps.

Lemme:
Sur k $q_1(x)$, $q_2(x)$ anisotropes sur k alors $q_1 \oplus T q_2$ l'est sur $k(T)$.

Plus généralement d'ailleurs, K val. disc avec car réd
π uniform, $q_1 \oplus \pi q_2$, q_1 et q_2 avec des coeff dans $\mathcal{O}_K$ de réduction $\tilde{q}_1$ et $\tilde{q}_2$ anisotropes. Alors q est anisotrope.

Remarques:
Classifiant si

w_1 $\qquad H^2(K)=0$ $\quad$ (K fini)

w_1, w_2 $\qquad H^3(K)=0$ $\quad$ (ex: corps de nbres totalt imagin; corps de fctions d'une var sur un corps fini).

w_1, w_2, signatures aux places réelles (ou classes de Stiefel Whitney..) $\quad$ corps de nbres.

On peut se débarrasser des (-1) si q forme quadratique de rang paire $n = 2m$

$$w(q) = 1 + w_1(q) +$$

$$w'(q) = w(q) / w(h)^m \qquad h = <1,-1>$$

$$= w(q) / [1+(-1)]^m \qquad w(h) = \underset{H^0}{1} + \underset{H^1}{(-1)}$$

$$w'(q_1 + q_2) = w'(q_1)\, w'(q_2)$$

$w'(q) = 1$ si q hyperbolique.

$$(1+w_1'(q)+w_2'(q)+\dots)(1+m(-1)+m_2(-1)(-1)+\dots)$$
$$= 1+w_1(q)+w_2(q)+\dots \qquad m_2=\frac{m(m-1)}{2}$$

$$w_1'+m(-1)=w_1$$
$$w_2'+m(-1)w_1'+m_2(-1)(-1)=w_2 \quad \dots$$

d'où $\quad d'=(-1)^{m/2}\,d.$ $\quad d$ si $n\equiv 0 \bmod 4$

$\qquad -d$ si $n\equiv 2 \bmod 4$

Pour $n=2$ $\quad w_2'=w_2+(-1)(-1)+(-1)w_1$

$q=\langle\alpha,\beta\rangle \quad w_2'=(-\alpha)(-\beta)$ Clifford de $(-q)$.

$n=4$ $\quad w_1'=w_1$

$\qquad w_2'=[D_q]$

$F(=K)$ corps de car $\neq 2$

<u>Anneau de Witt</u> : $\longrightarrow$ <u>Grothendieck-Witt</u>

notation (fâcheuse !) GrW ou $\tilde{W}$.

$$[f]+[g]=[f\oplus g]$$

GrW universel pour les fctions de formes quad. à valeurs dans les groupes abéliens

$$f(q\oplus q')=f(q)+f(q').$$

produit = produit tensoriel.

<u>Anneau de Witt</u> $W=GrW/\mathfrak{a}$ $\quad\mathfrak{a}$ engendré par

$$h=\langle 1,-1\rangle$$

$$f_n\otimes h\simeq nh \qquad \langle\alpha,-\alpha\rangle=\langle 1,-1\rangle$$

"$W=W_F$" $=: GrW/\mathfrak{a}$.

On a $W_F \longrightarrow \mathbb{Z}/2\mathbb{Z} \to 0.$

rang mod 2

$I_F = \operatorname{Ker}[W_F \to \mathbb{Z}/2\mathbb{Z}]$ classes des formes de rg pair

I_F^m / I_F^{m+1} ? cf Inv. Math 1970.

Relations entre :

(a) I_F^m / I_F^{m+1} ...

(b) $H^m(F)$

(c) $k_m(F) = K_m^M(F) / 2K_m^M(F)$

Qu'est-ce que $K_*^M(F)$? anneau gradué, engendré par des élts de d° 1, relations de degré 2 ou 1.

$K_0^M(F) = \mathbb{Z}$

$x \in F^* \longmapsto \{x\} \in K_1^M F$ générat.

$\{xy\} = \{x\} + \{y\}$.

$\{x\}\{1-x\} = 0$ pour tout $x \neq 0, 1$ $x \in F$

$\{x_1\} \cdots \{x_n\} =: \{x_1, \dots, x_n\}$

On dispose de flèches

$$\begin{tikzcd} k_m F \arrow[r, "\alpha"] \arrow[dr, "\beta"'] & I_F^m / I_F^{m+1} \\ & H^m(F) \end{tikzcd}$$

flèches faciles à definir, α surjective.

<u>Conjecture</u> : Ce sont des <u>isomorphismes</u>

Si pour un corps F et un degré n, α et β isomorphism

$$\begin{tikzcd} k_n F \arrow[r, "\alpha"] \arrow[dr, "\beta"'] & I_F^n / I_F^{n+1} \arrow[d, "\bar{e}_F^n"] \\ & H^n(F) \end{tikzcd}$$

$\bar{e}_F^n : I^n / I^{n+1} \xrightarrow{\sim} H^n(F)$

On note $e_F^n : I^n \longrightarrow H^n(F)$.

Ds la littérature "e_F^n" existe s'il y a un homom $I^n \to H^n(F)$ trivial sur I^{n+1} et rendant le diagramme commutatif.

$k_1 F = F^* / F^{*2}$

$H^1(F) \simeq F^* / F^{*2}$

β $\{x\} \longmapsto (x) \in H^1(F)$

$\{x_1, \dots, x_n\} \longmapsto (x_1) \dots (x_n) \in H^n(F)$

$\{x\}\{1-x\} = 0$.

α: $\{x\} \longmapsto ? \in I_F / I_F^2$

$\langle x \rangle - \langle 1 \rangle$

forme quad à 1 variable; "$-$" (ds anneau de Witt)

forme de rg 0.

ou encore $\langle 1 \rangle + \langle -x \rangle$

les 2 formes sont égales mod I_F^2 :

$\langle x \rangle + \langle -x \rangle = 0$ ds W_F

$\underset{\underset{I_F}{\cap}}{2}(\langle 1 \rangle - \underset{\underset{I_F}{\in}}{\langle x \rangle}) \in I_F^2$

Il faut vérifier que $\{x\}\{1-x\} \to 0$

$(\langle 1 \rangle + \langle -x \rangle) \otimes (\langle 1 \rangle + \langle x-1 \rangle) = 0$.

$n=1$ $\quad$ $k_1F = F^*/F^{*2} \xrightarrow{\sim} I_F/I_F^2$

$$\begin{tikzcd} k_1F = F^*/F^{*2} \arrow[r, "\sim"] \arrow[dr, "2"'] & I_F/I_F^2 \\ & H^1(F) \end{tikzcd}$$

trivial !

$n=2$ $\quad$ $k_2F \xrightarrow{\sim} I_F^2/I_F^3$ (Milnor)

$$\begin{tikzcd} k_2F \arrow[r, "\sim"] \arrow[dr, "2"'] & I_F^2/I_F^3 \\ & H^2(F) \end{tikzcd}$$

Merkuriev ~ 1980

$n=3$ $\quad$ α, β isomorphismes

Merkuriev - Suslin $\quad$ preprint 1986

Rost $\quad$ — 1986

$n=4$ $\quad$ e_F^4 existe $\quad$ Jacob - Rost $\quad$ Inv. Math 96 1989

Shievski $\quad$ Dokl. 308 1989.

On peut aussi introduire F_q plus grande 2-ext. de F (ie ext gal. à grpe de Galois un pro-2-grpe)

$$\begin{array}{c} F_q \\ | \\ F \end{array}$$

$Gal(F_q | F)$ = plus grand pro-2-quotient de G_F $:= G_F(2)$

$$H^n(G_F(2)) \xrightarrow{\text{inf.}} H^n(F)$$

$$\| $$

$$H^n_q(F)$$

("cohomologie quadratique de F")

Si $\alpha : k_n \longrightarrow I^n/I^{n+1}$

$\beta \quad k_n \longrightarrow H^n$

Si les β sont surjectifs (en dim $\leq n$) alors $H^n_q(F) \to H^n(F)$ est un isom.

En effet surj de $\beta \Rightarrow [H^1(F)=0 \Rightarrow H^i(F)=0 \quad \forall i \geq 1]$.

car surj de $\beta \Rightarrow H^i(F)$ est engendré par les cup produits des élts de H^1

$H^1(F(2)) = 0. \Rightarrow H^i(F(2)) = 0$

$$\begin{array}{l} k^n_F \longrightarrow I^n_F / I^{n+1}_F \\ \downarrow \\ H^n_q(F) \\ \downarrow \\ H^n(F) \end{array}$$

Conjecturalement, toutes les flèches sont des isomorphism

q, q' formes de rang n

$w_1(q) = w_1(q')$

$w_2(q) = w_2(q') \longrightarrow i(q,q') \in H^3(K)$

$Q = q \oplus (-q')$ rang $2n$ pair

$Q \to [Q] \in I_F$

Lemme $[Q] \in I^3_F$

~~$w'(-q) = \dfrac{1}{w'(q)}$ car $q \oplus -q$ hyp.~~

Soit $w'(q)\, w'(-q) = 1$.

~~$w'(Q) = w'(q) / w'(q')$~~

i.e $w'_1(Q) = 0 \quad w'_2(Q) = 0$.

$I^3_F / I^4_F \simeq H^3(F)$

$i(q,q') = $ image ds $H^3(F)$

Thme Si $n \leq 7$, si q, q' sont tels que $w_i(q) = w_i(q')$, $i = 1, 2$ et $i(q,q') = 0$, alors $q \sim q'$.

Thme (Arason - Pfister) Si Q est de rang $< 2^n$ et app $\bar{a}$ I_F^{n+1}, alors Q est hyperbolique.

$Q = q \oplus -q'$ $\quad n = 4 \ldots$

cf Lam ou l'article original de Pfister

$Q \in I^3$ $\quad i(q,q') = $ image de Q ds I^3 / I^4

donc $Q \in I^4$, donc hyperbolique, ie $q \sim q'$

Rque i est un invariant relatif

si q rg 4 dis $\square$ $\quad i(q) =: i(\alpha \text{ Norme}, \text{Norme})$

q α Norme.

mais en général...

Cohomologie du groupe orthogonal ; le groupe $\tilde{O}(q)$

K corps de base

q de rang n

O(q) gr. orthogonal de q.

$$\to SO(q) \to O(q) \to \{\pm 1\} \to 1$$

$$\begin{array}{ccc}
(\pm 1) & & \{\pm 1\} \\
\downarrow & & \downarrow \\
Spin(q) & \text{revêt}^{t} \text{ univers à 2 feuillets simpl}^{t} \text{ connexe} \quad \subset & \tilde{O}(q) \\
\downarrow & & \downarrow \\
SO(q) & \subset & O(q) \\
\downarrow & & \downarrow \\
1 & & 1
\end{array}$$

On peut associer canoniq^t à q un revêt^t à 2 feuillets redonnant le gpe des spineurs sur SO.

Si $q \to \lambda q$, $SO(q) = SO(\lambda q)$, $Spin(q) = Spin(\lambda q)$, mais $\tilde{O}(\lambda q) \neq \tilde{O}(q)$.

$C = C(q) =$ alg. de Clifford de q

V ev. sur lequel q est défini $\quad q(x) = x.x$

C eng. par V avec les relations ↓ pour tout $x \in V$

$\Rightarrow x.y = -yx$ si ~~o~~ x et y ⊥ pour q.

$\dim C = 2^n \quad n = \text{rang } q = \dim V$

antiautom $x \mapsto x'$ de C caractérisé par $x' = x$ si $x \in V$.

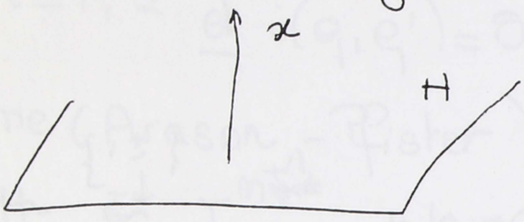
$$(x_1 \dots x_k)' = x_k \dots x_1 \qquad x_i \in V$$

Remarque

Soit $x \in V$ $q(x) = 1$ (d'où $x^2 = 1$ ds C, $x' = x$)

$x = x^{-1}$

$y \in V$ $\quad xyx^{-1} = xyx = \begin{cases} y & \text{si } y \text{ multiple de } x \\ -y & \text{si } y \in H \end{cases}$



H = orth. de x.

$xyx = -xxy = -y$

$y \longmapsto -xyx^{-1}$ est la symétrie par rapport au plan H

Après agg. du corps de base ($\to$ "$x^2 = 1$"), tout est obtenu comme cela

$C = C^+ \oplus C^-$ $\quad C^+$ eng. par les produits pairs $x_1 \ldots x_{2n}$ $x_i \in V$

C^- ——— impairs

C^+ paire / C^- impair

$\mathrm{Spin} = \{ z \in C^+,\ zz' = 1,\ zVz^{-1} = V \} = \tilde{O}(q)_+$

$\tilde{O}(q)_- = \{ z \in C^-,\ \text{———},\ \text{———} \}$

K Groupes algébriques sur K

$\tilde{O}(q)$, ... $\quad (\tilde{O} = \tilde{O}_+ \cup \tilde{O}_-)$.

Ces groupes ont les propriétés voulues

A définir

$\tilde{O}(q)_+ \longrightarrow SO(q)$

Ψ

z $\qquad v \mapsto zvz^{-1} \in SO(q)$

$\tilde{O}(q)_- \longrightarrow O(q) - SO(q)$ $\quad v \mapsto -zvz^{-1}$

$$1 \longrightarrow \pm 1 \longrightarrow \tilde{O}(q)_+ \rightarrow SO(q) \rightarrow 1$$

comme suite exacte de gpes algébriques (pas exact bien sûr sur le corps de base !).

$$1 \longrightarrow \pm 1 \longrightarrow \tilde{O}(q)_* \longrightarrow O(q) \rightarrow 1 .$$

S'il y a des vecteurs de carrés 1 pour q, on en choisit un, $O(q) = SO(q) \rtimes (1, \sigma)$

σ réflex. / hyp perpend.

$$\tilde{O}(q) = Spin(q) \rtimes (1, \sigma)$$

4/2/91

(Bruno Kahn)

I <u>Formes de Pfister</u>

$(x_1^2+x_2^2)(y_1^2+y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2+x_2y_1)^2$

$(x_1^2+\dots+x_4^2)(y_1^2+\dots+y_4^2) = (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \dots$

N polynôme homogène de degré d en n var $/F$, car $F \neq 2$

(0) $N^{-1}(\{0\}) = \{0, \dots, 0\}$

(1) E/F extension $N(E^n) - \{0\}$ est un sous-groupe de E^*

ex: $N = \Sigma$ de $2\,\square$, $4\,\square$, $8\,\square$

si $E = F(X_1, \dots, X_n, Y_1, \dots, Y_m)$ (2) formule $N(\vec{X})N(\vec{Y}) = N(\phi(\vec{X}, \vec{Y}))$

avec $\phi_i(\vec{X}, \vec{Y}) \in E$.

(fractions rationnelles)

Rque: L'inverse est facile! $N(x)^{-1} = \dfrac{N(x)^{d-1}}{N(x)^d}$

et par homogénéité $= N\left(\dfrac{x}{N(x)}\right)$

si $\vec{\phi}$ peut être donné par des polynômes, alors $N = N_0^i$ avec

$N_0 = N_{E/F} \circ Nrd_D$ $[E:F] < \infty$ D corps gauche de centre E

ou

$N_0 = N_{E/F} \circ \nu_0$ $[E:F] < \infty$ θ "corps" d'octonions de centre E, ν_0 norme de θ.

Il n'y a rien d'autre: $\vec{\phi}$ donné par des polyn. homog. d'où donné par loi d'algèbre, si tordue convenablement avec élts neutres à gche et dte; c'est forcément alternative et ces algèbres sont classifiées.

et on autorise les dénominateurs

si $d = 2$ il y en a d'autres les formes de Pfister

Notation $n \geq 1$ $a_1, \dots, a_n \in F^*$

$$\langle\langle a_1, \dots, a_n \rangle\rangle = \langle 1, -a_1 \rangle \otimes \dots \otimes \langle 1, -a_n \rangle$$

c'est une n-forme de Pfister.

⚠ notation ss signe − existe ds la littérature

Théorème (Pfister) φ forme quadratique anisotrope

Cond. équiv.

(1) E/F extension qqe, $\varphi(E^n) - \{0\}$ est un gpe

(2) φ est multiplicative avec $\varphi(\vec{x})\varphi(\vec{y}) = \varphi(\vec{\phi}(\vec{x}, \vec{y}))$

(3) $\exists \vec{\phi}$ linéaire en $\vec{y}$ avec (2)

(4) φ est une forme de Pfister

(cf Lam, Ch X)

On va donner une dém constructive de (4) $\Rightarrow$ (1) et (3)

Par récurrence sur n.

$$\varphi = \varphi_{n-1} \otimes \langle\langle a_n \rangle\rangle = \varphi_{n-1} \perp -a_n \varphi_{n-1}$$

W espace vect ss jacent à φ_{n-1}

$$V = W \oplus W.$$

φ_{n-1} forme de Pfister donc multiplicative

$x \in W$ $\exists u_x \in GL(W)$ $\varphi_{n-1} \circ u_x = \varphi_{n-1}(x)\varphi$.

A dém. $x \in V$ $\exists u_x \in GL(V)$ $\varphi \circ u_x = \varphi(x)\varphi$.

$$x = \underset{W}{x_0} + \underset{W}{x_1} \qquad u_x = \begin{pmatrix} u_{x_0} & a_n u_{x_1} \\ u_{x_1}^* & v \end{pmatrix} \quad v\,? \in \mathrm{End}_F W$$

$u_{x_1}^*$ adjoint

i) $x_1 = 0$. on prend $v = u_{x_0}$.

ii) $x_1 \neq 0$. φ_{n-1} anisotrope on peut diviser par ses valeurs

$$v = u_{x_1}^{-1} u_{x_0}^{*} u_{x_1}$$

N.B $\quad \det u_{x_1} = \varphi_{n-1}(x_1)^{2^{n-1}}$

$$\det u_x = (\det u_{x_1})^{2^{n-1}} \det(u_{x_0}) \det(u_{x_0})$$

$$\det(u_{x_0}) = \varphi_{n-1}(x_0)^{2^{n-2}}$$

Pour 16 variables par exemple:

$$x_1^2 + \dots + x_{16}^2 \xrightarrow{\det} (x_1^2 + \dots + x_8^2)^4$$

$$x_1^2 + \dots + x_{32}^2 \longrightarrow (x_1^2 + \dots + x_{16}^2)^{24} (x_{17}^2 + \dots + x_{24}^2)^4$$

Application Artin Schreier Si F n'est pas ordonnable, alors -1 est somme de carrés de F.

$s(F)$ = plus petit nbre de $\square$ nécessaires

<u>Corollaire</u> $s(F)$ <u>est une puissance de 2</u>

Dem $\quad -1 = x_1^2 + \dots + x_s^2 \qquad s = s(F)$

$$(\Rightarrow \forall i_1 < \dots < i_r \quad x_{i_1}^2 + \dots + x_{i_r}^2 \neq 0)$$

$$2^n \leq s < 2^{n+1}$$

$$\underbrace{x_1^2 + \dots + x_{2^n}^2}_{a} + \underbrace{x_{2^n+1}^2 + \dots + x_s^2 + 1}_{b} = 0$$

Notation φ forme quadratique

$$D_F(\varphi) =: \{\varphi(x) \mid x \in F^n\} - \{0\}$$

Ici a et b sont representés par φ: $D_F(x_1^2 + \dots + x_{2^n}^2) \ni a, b$

D_F est un groupe

$$-1 = \frac{a}{b} \in D_F(x_1^2 + \dots + x_{2^n}^2)$$

Théorie des formes de Pfister

Prop : I_F^n est engendré additivement par les n formes de Pfister.

I_F =: idéal de l'anneau de Witt tq correspond au noy. de l'augmentation
$= \mathrm{Ker}\,(W(F) \xrightarrow{rg} \mathbb{Z}/2\mathbb{Z})$

Propriété : Si une forme de Pfister est isotrope, elle est hyperbolique

$$\varphi = \varphi_{n-1} \otimes \langle\langle a_n \rangle\rangle = \varphi_{n-1} \perp -a_n \varphi_{n-1}$$

Il existe $a, b \in D_F(\varphi_{n-1})$ tq $a - a_n b = 0$

$$a_n = \frac{a}{b} \in D_F(\varphi_{n-1})$$

$$\varphi = \varphi_{n-1} \perp -a_n \varphi_{n-1} \simeq \varphi_{n-1} \perp -\varphi_{n-1} \text{ hyperbolique}$$

Corps de fonctions

q forme quadratique de rg N V. $N \geq 3$ ou $N = 2$ et q anisotrope

X_q = variété des zéros de q $\begin{cases} \text{affine} \\ \text{projective} \end{cases}$

$F(q)$ = corps de fctions de la variété affine

$d^o \mathrm{tr}\, F(q) = N-1$

(cas projectif $N-2$)

Autre description : $F(q)$ ne dépend que de la classe de similitude de q. $\rightarrow$ On peut supposer q représente.

$$q = \langle 1 \rangle \perp -\underset{x_2, \dots, x_n}{q'} \qquad F(q) = F(x_2, \dots, x_n, \sqrt{q'(x_2, \dots, x_n)})$$

ie extension quadratique d'une transc. pure

Prop. $q \otimes_F F(q)$ est isotrope

$F(q)/F$ est transc. pure $\Leftrightarrow$ q isotrope sur F

$\Leftarrow$ $q = xy \perp$?

$\Rightarrow$ Lemme q anisotrope $/F$

$q \otimes^F F(q)$ est anisotrope

Si φ est de Pfister $\Rightarrow$ $\varphi \otimes_F F(\varphi)$ est hyperbolique

Lemme 1 $E = F(\sqrt{a})$ $\quad \mathrm{Ker}\,(W(F) \to W(E)) = \langle\langle a \rangle\rangle W(F)$

$W(F), W(E)$ anneaux de Witt

q anisot. $/F$ $\quad q \otimes E$ isotrope $\Rightarrow$ $\underbrace{q > \lambda \langle\langle a \rangle\rangle}_{\text{contient une ss forme.}}$

$\varphi' > \varphi \Rightarrow \exists \varphi_1$ tq $\varphi' \simeq \varphi \perp \varphi_1$

Lemme 2 (Pfister) φ, ψ deux formes quadratiques avec ψ anisotrope.

Si $\varphi(\vec{x}) \in D_{F(\vec{x})}(\psi)$, alors $\psi > \varphi$

Theorème φ, ψ deux formes quad. ψ anisotrope

$\dim \varphi > 1$

Hypoth: $\psi \otimes_F F(\varphi)$ hyperbolique

a) Si $\varphi = \psi$ alors φ est semblable à une forme de Pfister

b) En général, $\exists a \in F^*$ tq $\psi > a\varphi$

c) Si φ est de Pfister, $\psi \simeq \varphi \otimes \theta$

ie $\mathrm{Ker}(W(F) \to W(F(\varphi))) = \varphi W(F)$

Démonstration

$\varphi = \langle 1 \rangle \perp \varphi'$

$\psi \otimes_F F(\varphi) = \psi \otimes_{F(x_2,\dots,x_n)} F(x_2,\dots,x_n,\sqrt{\varphi'(x_2,\dots,x_n)})$

hyperbolique

$\Longrightarrow \varphi'(x_2,\dots,x_n) \in D_{F(x_2,\dots,x_n)}(\psi)$

$\psi \simeq_{F(x_2,\dots,x_n)} \langle\langle \varphi'(x_2,\dots,x_n) \rangle\rangle \otimes \theta$

$\Longrightarrow \varphi^*(x_1,x_2,\dots,x_n) \cdot \psi \simeq \psi$ sur $F(x_1,\dots,x_n)$

dans le cas a) φ est multiplicative, donc de Pfister

b) $\exists a \in F^*$

$a\varphi(x_1,\dots,x_n) \in D_{F(x_1,\dots,x_n)}(\psi) \Rightarrow \psi > a\varphi$

Théorème d'Arason-Pfister ($\sim$ 1971)

q forme quadratique de rang $< 2^n$

On suppose que $[q] \in I^nF$

Alors q est hyperbolique.

Notation $q \sim q'$: $\exists h_1, h_2$ hyperboliques. $q \perp h_1 \simeq q' \perp h_2$

$q \sim \varepsilon_1\varphi_1 + \dots + \varepsilon_r\varphi_r \quad \varepsilon_i = \pm 1 \quad \varphi_i$ n formes de Pfister.

On raisonne par récurrence sur r

Si φ_r non hyp., φ_r anisotrope

$q \otimes_F F(\varphi_r) = \varepsilon_1\varphi_1 + \dots + \varepsilon_{r-1}\varphi_{r-1}$ est hyperbolique

Si q non hyperb, $q_{an} = \varphi_n \otimes ? \Rightarrow rg\, q_{an} \geq 2^n$ exclu

Invariant cohomologique

$a_1, \dots, a_n \in F^* \longmapsto \{a_1, \dots, a_n\} \in k_n F = K_n^M F/2$

Thme (Arason) Cela ne dépend que de $\langle\langle a_1, \dots, a_n \rangle\rangle$.

Corollaire $(a_1, \dots, a_n) \in H^n F = H^n(F, \mathbb{Z}/2)$ ne dépend que de $\langle\langle a_1, \dots, a_n \rangle\rangle$.

$(a_1, \dots, a_n) =: (a_1) \cup \dots \cup (a_n)$

(a_i) classe ds H^1 via Kummer

$\cup$ cup produit.

Démonstration

$\underbrace{\langle a_1, \dots, a_n \rangle \simeq \langle b_1, \dots, b_n \rangle}_{\text{en chgt 2 entrées à la fois}}$

Pour les formes de Pfister

lemme (Arason): Si $\varphi = \langle\langle a_1, \dots, a_n \rangle\rangle \simeq \langle\langle b_1, \dots, b_n \rangle\rangle$

alors $\exists c \in F^*$ tq $\varphi = \langle\langle a_1, \dots, a_{n-1}, c \rangle\rangle = \langle b_1, \dots, b_{n-1}, c \rangle$

D'où :

$\langle\langle a_1, \dots, a_n \rangle\rangle = \langle\langle a_1, \dots, a_{n-1}, c \rangle\rangle$

$\langle\langle a_1, \dots, a_{n-1} \rangle\rangle \perp -a_n \langle 1 \rangle = \langle\langle \quad \rangle\rangle \perp c \langle\langle \quad \rangle\rangle$.

$a_n \in D_F(\langle\langle a_1, \dots, a_{n-1} \rangle\rangle)$

$\{a_1, \dots, a_n\} = \{a_1, \dots, a_{n-1}, c\} + \{a_1, \dots, a_{n-1}, x\}$.

Lemme $x \in D_F(\langle\langle a_1, \dots, a_{n-1} \rangle\rangle) \Rightarrow \{a_1, \dots, a_{n-1}, x\} \in 2K_n^M$

Alors $\{a_1, \dots, a_n\} \equiv \{a_1, \dots, a_{n-1}, c\}$

$\{b_1, \dots, b_n\} \equiv \{b_1, \dots, b_{n-1}, c\}$.

Corollaire du 1er lemme : on peut passer d'une écriture à l'autre en ne chgt qu'une entrée à la fois $\rightarrow$ ce qu'on veut

Dém du 2^e lemme pour $n=2$

$$x = x_0^2 - a_1 x_1^2$$

$$\{a_1, x_0^2 - a_1 x_1^2\} = \{a_1 \frac{x_1^2}{x_0^2}, 1 - a_1 \frac{x_1^2}{x_0^2}\} = 0$$

(relation de Steinberg).

Dém. du lemme d'Arason

$$\varphi_1 = \langle\langle a_1, \dots, a_{n-1} \rangle\rangle = 1 \perp \varphi_1' \qquad \varphi_2 = \langle\langle b_1, \dots, b_{n-1} \rangle\rangle = 1 \perp \varphi_2'$$

Hypothese $\varphi_1 \otimes \langle\langle a_n \rangle\rangle \perp -\varphi_2 \otimes \langle\langle b_n \rangle\rangle$ est hyperbolique

$$\theta = (\varphi_1' \perp -\varphi_2') \perp (a_n \varphi_1 \perp -b_n \varphi_2) \sim 0$$

Remarque θ forme hyperbolique de rang $2N$, $\rho < \theta$

$\operatorname{rg} \rho > N \Rightarrow \rho$ est isotrope

$$\Longrightarrow \exists c = a_n \varphi_1(\vec{x}) = b_n \varphi_2(\vec{y})$$

$$\langle\langle a_1, \dots, a_n \rangle\rangle = \langle\langle a_1, \dots, a_{n-1} \rangle\rangle \perp c\, \varphi_1(\vec{x})^{-1} \varphi_1$$

$$\simeq \langle\langle a_1, \dots, a_{n-1} \rangle\rangle \perp -c\varphi_1 = \langle\langle a_1, \dots, a_{n-1}$$

$$\begin{tikzcd}
 & I_F^n / I_F^{n+1} \arrow[dd, dashed, "?\ e_F^n"] \\
k_m F \arrow[ur] \arrow[dr] & \\
 & H^n F
\end{tikzcd}$$

$\{a_1, \dots, a_n\} \mapsto \langle\langle a_1, \dots, a_n \rangle\rangle$, $\{a_1, \dots, a_n\} \mapsto (a_1, \dots, a_n)$

Arason (Elman-Lam) $\varphi_1 \perp \varphi_2 \equiv \varphi_3 \mod I_F^{n+1}$

$\varphi_1, \varphi_2, \varphi_3$ n-formes de Pfister $\Longrightarrow e_F^n(\varphi_1) + e_F^n(\varphi_2) = e_F^n(\varphi_3)$

Thme (Arason) e^3_F <u>est bien défini</u> $\forall F$
Thme (Jacob - Rost, Suslin) e^4_F <u>idem</u>

<u>Remarque</u> (Milnor)

$$w_{2^{n-1}}(\langle\langle a_1, \ldots, a_n\rangle\rangle') = \underset{-1 \text{ dans } H_1}{\{-1\}}^{2^{n-1} * n} e^n_F(\langle\langle a_1, \ldots, a_n\rangle\rangle)$$

Arason montre que e^n_F est bien défini $\forall F$ si $\forall F$ φ forme quadratique de rang $> 2^n$ $H^nF \hookrightarrow H^nF(\varphi)$

$n = 1$ $\quad H^1F \not\hookrightarrow H^1F(\varphi)$ si F n'est pas algt fermé ds $F(\varphi)$
$\Rightarrow rg\, \varphi = 2$.

$n = 2$ $\quad \alpha \in Ker(H^2F \to H^2F(\varphi)) - \{0\}$
$\alpha = [D] \quad D_{F(\varphi)} \sim 0$
Mais $F(\varphi)$ est une extension transcendante pure de F.
$\Rightarrow D$ est un corps de quaternions $\left(\frac{a\ b}{F}\right)$
$\left(\frac{a\ b}{F(\varphi)}\right) \sim 0 \Rightarrow \langle\langle a, b\rangle\rangle_{F(\varphi)} \sim 0$
$\Rightarrow \varphi < \langle\langle a, b\rangle\rangle$
$rg\, \varphi \leq 4$

Thme (Arason) φ $rg\, \varphi > 2$, φ <u>anisotrope</u>
<u>Il existe</u> $\alpha \in Ker(H^3F \to H^3F(\varphi)) - \{0\}$
$\alpha = (a, b, c)$ et $\lambda\varphi < \langle\langle a, b, c\rangle\rangle$
$\lambda \in F^*$ $(\Rightarrow rg\, \varphi \leq 8)$.
(a, b, c) convenable et λ convenable

Thme (Jacob-Rost) φ 4-forme de Pfister

$\mathrm{Ker}(H^4(F) \to H^4(F(\varphi))) = e^4_F \varphi \cup H^0 F$

suffit à montrer l'existence de e^4_F.

Conjecture de Kato :

F $\quad K^M_n F / m \longrightarrow H^n(F, \mu_m^{\otimes n})$

$(m, \mathrm{car} F) = 1$

$n = 1$ théorie de Kummer

$n > 1$ cup produit

C'est un isomorphisme

$m = 2$ (ex : conjecture de Milnor)

Cas connus

Thme (Merkurjev - Suslin) C'est un isomorphisme

si $n = 2$

Thme (Rost - Merkurjev - Suslin) C'est un isomorphism

si $n = 3$ et $m = 2^r$

Thme (?) ~~Rohs~~ Rost : idem avec $n = 4$ et $m = 2^r$

(non rédigé).

11/2/91.

$O(q)$

q f. quad. non dégénérée de rang $n \geq 1$

$$\begin{array}{ccccccccc} & & \mathrm{Spin}(q) & \longrightarrow & \tilde{O}(q) & & & & \\ & & \downarrow & & \downarrow & & & & \\ 1 & \longrightarrow & SO(q) & \longrightarrow & O(q) & \xrightarrow{\det} & \{\pm 1\} & \longrightarrow & 1 \end{array}$$

ext. centrale $\left(\begin{array}{c}\text{non triviale} \\ \text{si } n \geq 2\end{array}\right)$ par $\{\pm 1\}$

Si $n \geq 3$, $\mathrm{Spin}(q)$ est le revêtement universel de $SO(q)$

$\tilde{O}(q)$ grpe algébrique

pts sur K

$C(q)$ = algèbre de Clifford

$C = C^+ \oplus C^-$

$x \mapsto x'$ anti-involution $\quad x \in V \Rightarrow x' = x$

$\mathrm{Spin}(q)$ = élts $x \in C^+$, $xVx^{-1} = V$, $xx' = 1$

$v \longmapsto xvx^{-1}$.

$\tilde{O}(q)^- = \tilde{O}(q) - \mathrm{Spin}(q) = \{x \mid x \in C^-, xVx^{-1} = V, xx' = 1$

$x \mapsto (v \longmapsto -xvx^{-1})$ signature -1

Il est possible bien sûr que ceci soit vide sur K.

Cas $n = 1$

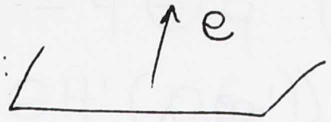
$SO = \{1\} \qquad q(x) = \alpha x^2 \qquad \alpha \in K^*$

$\mathrm{Spin} = \{\pm 1\}$

$1 \longrightarrow \mathrm{Spin} \longrightarrow \tilde{O} \longrightarrow \{\pm 1\} \longrightarrow 1$

Si K assez grand (en fait, si $\alpha = \square$ de K),

il y a des pts rationnels de $\tilde{O}$ se projetant sur -1.

cas symétrie:  $e^2 = 1$

Ds ce cas $\hat{O}(q)$ gpe de type $(2,2)$ formé de pts rationnels $/K$.

Action galoisienne du type unipotent $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, ie donnée par $G_K \to \mathbb{Z}/2\mathbb{Z}$; le caractère correspondt est $(\alpha) \in H^1(G, \mathbb{Z}/2\mathbb{Z})$.

En particulier, multiplier q par une constante chge l'action galoisienne (donc $\hat{O}(q)$).

Ex : Faire tout ceci explicitement...

w_1 $\quad$ q forme quadratique

w_2 $\quad$ $n \geq 1$ rang

$\alpha \in H^1(K, O(q))$

q_α forme tordue par α.

On veut calculer les invariants w_1, w_2 de q_α en fction de α et de ceux de q.

$$O(q) \xrightarrow{\det} \{\pm 1\} \to 1$$

$$\alpha \in H^1(K, O(q)) \longrightarrow H^1(K, \{\pm 1\}) = H^1(K)$$

$$\alpha \longmapsto \delta^1(\alpha) \in H^1(K)$$

D'autre part, suite exacte de gpes algébriques :

$$1 \to \{\pm 1\} \to \hat{O}(q) \to O(q) \to 1$$

$$\Delta : H^1(K, O(q)) \longrightarrow H^2(K) \qquad \text{cobord.}$$

$$\alpha \longmapsto \Delta\alpha := \delta^2(\alpha).$$

Théorème :

$$w_1(q_\alpha) = w_1(q) + \delta^1(\alpha)$$

$$w_2(q_\alpha) = w_2(q) + w_1(q)\cdot\delta^1(\alpha) + \delta^2(\alpha)$$

Ou encore $1 + w_1(q_\alpha) + w_2(q_\alpha) + \dots \equiv (1 + w_1(q) + \dots)(1+\delta^1(\alpha)+$

mod termes de $d^o \geq 3$

Si classe de cohomol. est ds $SO(q)$, la formule se simpl~~emei~~fie ... (et se trouve ds la littérature)

Corollaire si $q =$ forme $\langle 1, \dots, 1 \rangle$

$$w_1(q_\alpha) = \delta^1(\alpha); \quad w_2(q_\alpha) = \delta^2(\alpha).$$

Démonstration : • Si formule vraie pour 2 formes quadratiques, vraie pr somme directe ;

• vraie en dim 1.

? vraie en dim 1 : $w_2(q_\alpha) = w_2(q) = 0$.

A vérifier $\delta^2(\alpha) = w_1(q).\ \delta^1(\alpha)$.

$q = ax^2 \qquad w_1(q) = (a) \in H^1(K)$

$\alpha \in H^1(O(q)) \simeq H^1(K)$

$q_\alpha = \langle a\alpha \rangle$

$$1 \to \pm 1 \to \tilde{O} \to \pm 1 \to 1, \text{ d'où}$$

$$H^1(K) \to H^1(K, \tilde{O}) \to H^1(K) \xrightarrow{\Delta} H^2(K)$$

L'action de Galois sur $\tilde{O}$ est attachée au caractère (a).

On a déjà trouvé une formule donnant le cobord ds le cas d'une telle action, à partir de la suite avec action triviale $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to$

c'est celle qu'on veut !

$q = q' \oplus q''$ $(= q' \perp q'')$

$\alpha' \in H^1(O(q'))$

$\alpha'' \in H^1(O(q''))$ $\alpha = \alpha' \perp \alpha'' \in H^1(O(q))$ en utilisant $O(q') \times O(q'') \hookrightarrow O(q)$.

? Formules $\delta^1(\alpha) = \delta^1(\alpha') + \delta^1(\alpha'')$

lemme : $\delta^2(\alpha) = \delta^2(\alpha') + \delta^1(\alpha')\,\delta^1(\alpha'') + \delta^2(\alpha'')$

Comme tjrs, la 1ère est évidente. Pour la 2e

$$\tilde{O}(q') \times \tilde{O}(q'') \xrightarrow{?} \tilde{O}(q) \quad (\triangle \text{ pas injectif!})$$

$$\downarrow$$

$$O(q') \times O(q'') \hookrightarrow O(q)$$

$\tilde{O}(q') \hookrightarrow \tilde{O}(q)$
$\tilde{O}(q'') \nearrow$

(mais pb du produit à cause de la commutation)

Si $g \in \tilde{O} \to O \xrightarrow{\det} (\pm 1)$

$\varepsilon(g) = \pm 1$ image ds ± 1

Si g et g' st ds $\tilde{O}(q')$, $\tilde{O}(q'')$ avec l'un des 2 pairs ils commutent, si ts les 2 st impairs, ils anticommutent.

(se voit par exemple sur les symétries).

Calcul du cobord.

$\delta^2(\alpha)$ α' repr. par $s \mapsto a'_s \in O(q')$, $s \in G_K$

On doit choisir $b'_s \in \tilde{O}(q')(K_s)$.

$\delta^2\alpha'$ repr. par le 2 cocycle.

$$(s,t) \longmapsto b'_s\, {}^s b'_t\, b_{st}^{-1} \in \{\pm 1\}_{q'}$$

α'' a''_s, b''_s $a_s = (a'_s, a''_s) \in O(q' \oplus q'')$

$b_s = b'_s \cdot b''_s$ (le produit étant calculé ds $\tilde{O}(q)$)

$\delta^2\alpha$ représenté par le 2-cocycle $(s,t) \mapsto b'_s\, b''_s\, {}^s b'_t\, {}^s b''_t \cdot b''^{-1}_{st}\, b'^{-1}_{st}$

$\varepsilon(b''_s) \in \mathbb{Z}/2\mathbb{Z}$

$$(s,t) \longmapsto (-1)^{\varepsilon(b''_s)\varepsilon(b'_t)}\ b'_s\,{}^s b'_t\,\underbrace{(b''_s\,{}^s b''_t\, b''^{-1}_{st})}_{\text{cobord de " ds le centre}}.\,b'^{-1}_{st}$$

$$u.v'.v''$$

avec $u = (-1)^{\varepsilon(b''_s)\varepsilon(b'_t)}$

$v' = b'_s\,{}^s b'_t\, b'^{-1}_{st}$

$v'' = b''_s\,{}^s b''_t\, b''^{-1}_{st}$

" $\varepsilon(b''_s) = \varepsilon(a''_s)$ " et " $\varepsilon(b'_t) = \varepsilon(a'_t)$ "

d'où la formule voulue.

Fin de la démonstration du thme sur la torsion

Récurrence sur n = rang.

Vrai si $n = 1$.

$n \geq 2$ on choisit une décomposition $q = q' \oplus q''$

avec rang $q' > 0$ et rang $q'' > 0$.

Or: $H^1(O(q') \times O(q'')) \to H^1(O(q))$ est surjectif.

Plus généralt (ε_i) base orthogonale de q

$$\underset{O(1)\times \overset{n}{\cdots} \times O(1)}{(\pm 1)^n} \hookrightarrow O(q)$$

et $H^1((\pm 1)^n) \to H^1(O(q))$ est surjectif

$\alpha = (\alpha_1, \ldots, \alpha_n) \in K^*/K^{*2}$

$q = \langle a_1, \ldots, a_n \rangle$ $\qquad q_\alpha = \langle a_1\alpha_1, \ldots, a_n\alpha_n \rangle$

on trouve donc tout !

Remarque

octaves de Cayley

$e_0 = 1$

e_i i mod 7

$(\pm 1)^3 \nearrow G_2$

$e_1 \longmapsto \pm e_1$

$H^1(K,(\pm 1)^3) \to H^1(K, G_2)$ surjectif.

$e_2 \longmapsto \pm e_2$ fixe le reste

$e_3 \longmapsto \pm e_3$

(Les 3-formes de G_2 st classées par les 3 formes de Pfister que l'on attrape avec le "petit" groupe). ∎

On peut supposer $\alpha = \alpha' \perp \alpha''$

d'où $q_\alpha = q'_{\alpha'} \oplus q''_{\alpha''}$

$$w(q_\alpha) = w(q'_{\alpha'}) \cdot w(q''_{\alpha''})$$

$$\equiv w(q') \cdot (1+\delta^1(\alpha')+\delta^2(\alpha'))$$

$$\cdot\, w(q'') \cdot (1+\delta^1(\alpha'')+\delta^2(\alpha'')) \quad (\text{mod deg } 3)$$

$$w(q_\alpha) \equiv w(q)\ (1+\delta^1(\alpha)+\delta^2(\alpha)) \quad \ldots$$

d'où le thme.

Remarques sur la caractéristique 2

On s'intéresse à q forme quadratique "non dégénérée" (donne quadrique lisse)

disc $\neq 0$ (si disc bien défini).

En dim paire sur K algr clos $\qquad x_1x_2 + \ldots + x_{2n-1}x_{2n}$

impaire $\qquad x_0^2 + x_1x_2 + \ldots + x_{2m-1}x_{2m}$

On va attacher à ces formes des invariants

$n = 2m \qquad O(q)$ lisse

composante neutre $SO(q)$

$$1 \to SO(q) \to O(q) \to \underset{\substack{\text{invariant}\\ \text{de Dickson}}}{\mathbb{Z}/2\mathbb{Z}} \to 0$$

Si $\alpha \in H^1(O(q)) \longrightarrow \delta^1(\alpha) \in H^1(\mathbb{Z}/2\mathbb{Z}) = K/\wp K$

$\wp x = x^2 + x$ en car 2.

définit l'invariant d'Arf ds H^1, à partir de la forme standart

Inv d'Arf trivial :

$$1 \to \mu_2 \longrightarrow Spin(q) \to SO(q) \to 1$$

~~Ce revêtement n'est pas~~ topo. étale ne donne pas ce qu'on veut

$$\alpha \in H^1(K, SO(q)) \longrightarrow \delta^2\alpha \in H^2_{fppf}(\mu_2) \simeq Br_2(K)$$

En dim paire, ttes les formes s'obtiennent comme

$$\alpha_1 x_1^2 + x_1x_2 + \beta_1 x_2^2 + \alpha_3 x_3^2 + x_3 x_4 + \beta_3 x_4^2 + \dots$$

~~et~~ $\delta^2\alpha = \Sigma [\alpha_i, \beta_i] \in Br_2(K)$ (à vérifier)

$n = 2m+1$ $O(q)$ pas lisse

$$1 \to \underset{\text{lisse}}{SO(q)} \to O(q) \xrightarrow{\text{dét}} \mu_2 \to 1.$$

en fait : $O(q) = \mu_2 \times SO(q)$

$\alpha \in H^1_{fppf}(O(q))$ $\quad$ dét $\alpha = \delta^1(\alpha) \in H^1_{fppf}(\mu_i) = K^*/K^{*2}$

$\delta^2(\alpha) \in Br_2(K)$.

---

car $K \neq 2$

$H^1(SO(q)) \xrightarrow{\alpha} H^1(O(q))$ injective $(n \geq 1)$

$$1 \to SO \to O \to \pm 1 \to 1$$

$$O(q)(K) \xrightarrow[\text{dét}]{} \{\pm 1\} \longrightarrow H^1(SO(q)) \xrightarrow[\alpha]{} H^1(O(q))$$

$O(q)(K) \to \{\pm 1\}$ surjective (réflections de déterminant -1).

$\alpha^{-1}(1) = (1)$ "injectivité naïve" (⚠ ce ne sont pas des groupes !).

Par torsion $H^1(SO(q)) \xrightarrow[\text{injectif}]{} H^1(O(q))$.

$$\begin{array}{c} H^1(K, Spin(q)) \\ \downarrow \\ H^1(K, SO(q)) \end{array}$$

on note $H^1(K, SO(q))_{spin}$ l'image de cette flèche

Soit $\alpha \in H^1(O(q))$, $\alpha \in H^1(SO(q)) \Leftrightarrow \delta^1(\alpha) = 0$.

$\alpha \in H^1(SO(q))_{spin} \Leftrightarrow \begin{cases} \delta^1(\alpha) = 0 \\ \delta^2(\alpha) = 0 \end{cases}$

$w_i(q_\alpha) = w_i(q) \quad i = 1, 2$

$\Updownarrow$

α est spinoriel.

On a une flèche canonique

$$H^1(K, SO(q))_{spin} \xrightarrow{i (= i_3)} H^3(K)$$
$$\alpha \in$$

$Q_\alpha = q_\alpha \oplus (-q)$

$[Q_\alpha] \in WK$ (gpe de Witt de K).

$W \supset I$ idéal d'augmentation $\supset I^2$

$W / I \simeq \mathbb{Z}/2\mathbb{Z}$ ($\leftrightarrow$ rg des formes mod 2)

$I / I^2 \simeq H^1(K)$

$Q_\alpha \longrightarrow 0$ ds I/I^2

$I^2/I^3 \simeq H^2(K)$ (Merkurjev-Suslin).

La classe α étant spinorielle, les w coïncident, d'où $Q_\alpha \in I^3$.

$I^3/I^4 \simeq H^3(K)$ (Rost, M.S)

On ne se sert en fait $I^3/I^4 \longrightarrow H^3(K)$

D'où $[Q_\alpha] \longrightarrow i_3(\alpha) \in H^3(K)$.

Si $i_3(\alpha) = 0$, alors on peut définir i_4 dans $H^4(K)$.

<u>L'invariant</u> i_3 :

- Si on remplace q par λq, $\lambda \in K^*$, alors $i_3(\alpha)$ ne change pas. En effet $O(\lambda q)$, $SO(\lambda q)$, $H^1(K, SO(\lambda q))_{spin}$ et resp. $O(q)$, $SO(q)$, $H^1(K, SO(q))_{spin}$

$Q_\alpha = q_\alpha \oplus -q$

$\lambda Q_\alpha = \lambda q_\alpha \oplus -\lambda q$

Si $Q \in I^n$, $\lambda Q \equiv Q \mod I^{n+1}$
car $\lambda Q - Q = (\lambda - 1) Q$ et $\lambda - 1 \in I$.

- $i_3(\alpha_1 \perp \alpha_2) = i_3(\alpha_1) + i_3(\alpha_2)$

$\alpha_1 \in H^1(K, SO(q_1))_{spin}$

$\alpha_2 \in$ ——

$\alpha_1 + \alpha_2 \in H^1(K, SO(q_1 + q_2))_{spin}$

$Q_{\alpha_1 \perp \alpha_2} = Q_{\alpha_1} \oplus Q_{\alpha_2}$

$i_3(\alpha_1 \otimes \alpha_2) = i_3(\alpha_1)\,\mathrm{rang}(\alpha_2) + i_3(\alpha_2)\,\mathrm{rang}(\alpha_1)$ (92)

Demonstration : $[q_{\alpha_1}] = [q_1] + \varepsilon_1 \qquad \varepsilon_1 \in I^3$

$i_3(\alpha) = $ classe de $q_\alpha - q \mod I^4$

$q_{\alpha_1} \otimes q_{\alpha_2} = q_1 \otimes q_2 + q_1 \otimes \varepsilon_2 + q_2 \otimes \varepsilon_1 + \varepsilon_1 \varepsilon_2$

On décompose q_1 en somme : $q_1 \otimes \varepsilon_2 = \underbrace{\varepsilon_2 + \cdots + \varepsilon_2}_{\mathrm{rg}\, q_1 \text{ fois}} \mod I^4$

Idem avec q_2

$\varepsilon_1 \varepsilon_2 \in I^6$ donne 0 ds I^4, qfd.

On veut appliquer ceci à la cohomologie galoisienne des gpes non orthogonaux, par exemple exceptionnels

$G \begin{cases} G_2 \\ F_4 \\ E_8 \end{cases}$ pas d'automorph. externe
pas de centre.

G sur K abst simple

$G \simeq \mathrm{Aut}\, G$

- Les représentations irréductibles de G sont réalisables sur K.

Après extension, poids dominant ω

V_ω irréd $\longleftrightarrow \omega$

En fait V_ω définissable sur K.

- Tres ces représent. st de type orthogonal.

On prend q_ω une forme quadratique non dégénérée invariante par G sur V_ω

d'où $G \longrightarrow SO(q_\omega)$ (car G connexe).

G simpl^t connexe, donc se relève

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\rho_\omega"'] & \mathrm{Spin}(q_\omega) \arrow[d] \\ & SO(q_\omega) \end{tikzcd}$$

Si $\alpha \in H^1(K, G)$, $\rho_\omega(\alpha)$ est spinorielle, d'où un $i_3(\rho_\omega \alpha)$
Ne dépend pas de q_ω

D'où pour tout poids dominant ω et tout $\alpha \in H^1(K,G)$, un élt $i_\omega(\alpha) \in H^3(K)$

Exemple $\quad G = G_2$

Partons de la forme déployée
$\omega = a\omega_1 + b\omega_2 \quad a, b \in \mathbb{N}$
ω_1, ω_2 représentations de d°7 et 14 respect.
(Octonions de trace 0) (rep. adjointe)

$\omega = \omega_1$: $\quad H^1(K, G_2) \xhookrightarrow{i} H^3(K)$

image formée des élts décomposables $(a)(b)(c)$, $(a), (b), (c) \in H^1(K)$

description par la 3-forme de Pfister

A démontrer : $i_{a\omega_1 + b\omega_2}(\alpha) = \begin{cases} 0 \\ i(\alpha) = i_{\omega_1}(\alpha) \end{cases}$ dépdt de a et b

Ex : $i_{\omega_2}(\alpha) \overset{?}{=} 0$, ie forme de Killing

$Kil_\alpha - Kil \in I^4$

Alors $i_4(Kil_\alpha - Kil) \overset{??}{=} (-3) \cdot i(\omega)$

$Kil_\alpha = \langle 1, -3 \rangle \otimes \varphi_7$

$1 \oplus \varphi_7 = \varphi_8$ (octonions)

ρ qqc $i_\rho(\alpha) \in H^3$

$i : R(G) \longrightarrow H^3(K)$

anneau des repr.

$i(\rho_1 \oplus \rho_2) = i(\rho_1) + i(\rho_2)$

$i(\rho_1 \otimes \rho_2) = i(\rho_1)\, \mathrm{rg}\, \rho_2 + i(\rho_2)\, \mathrm{rg}(\rho_1)$

$V_{\omega_1}, V_{\omega_2}$ engendrent $R(G_2)$, donc suffirait de connaître représent explicite .. (voir p. 111 bis)

18 février 1991

G_2, F_4, E_8 ss, simplement connexe

$\mathrm{Aut}\, G \simeq G$

Les repr. lin. de G sont "orthogonales"

— — "définies sur K"

Principe : H/K

$$H \xrightarrow{\rho} GL_n = GL(V)$$

$\alpha \in H^1(K, H)$. $H_\alpha \xrightarrow{\rho_\alpha} GL(V_\alpha) \simeq GL_n$

s'il y a une f.q. invariante, non dégénérée q

q_α est — " —.

ρ irréductible, repr. de G

$$H^1(K, G) \longrightarrow H^3(K) \qquad i_3(\rho, \alpha)$$

$\alpha \in H^1$

$\rho : G \longrightarrow SO$ (→ Spin), on choisit une f.q. invariante.

On a : $H^1(K, G) \longrightarrow H^1(K, SO)_{\text{spin}} \xrightarrow{i_3} H^3(K)$.

Repr. irréd. de G_2 dépendent de 2 paramètres m, n.

Le foncteur i_3 s'étend à toutes les ↑ représentations de G.

$\underline{\mathrm{car}\, K = 0}$

Soit ρ une repr. lin. de V.

$$V \simeq \bigoplus_{S \text{ irréd}} S \otimes W_s$$

W_s e.v. de dim $< \infty$ act. triv. de G.

$W_S = \mathrm{Hom}^G(S, V)$

q invariante sur V

S irréd.

q_S f. quad. inv. sur S

$$q = \bigoplus q_S \otimes \phi_S$$

ϕ_S : forme quadratique non. dég. sur W_S

On pose $\quad i_3(\rho, \alpha) = \sum_S \overbrace{\dim W_S}^{\text{ne compte que mod } 2} \cdot i_3(\rho_S, \alpha)$

$$\in H^3(K)$$

A voir :
clair aussi le i_3 associé à

$$H^1(K, G) \to H^1(K, SO(V, q))$$
$$\downarrow$$
$$H^3(K)$$

Ds $W(K)$

$n_S = \dim W_S$

$$(q_S \otimes \phi_S)_\alpha - (q_S \otimes \phi_S) \equiv (q_S \otimes n_S)_\alpha - (q_S \otimes n_S) \quad (\mathrm{mod}\ I^4)$$

où $\quad q_S \otimes n_S = q_S \oplus \cdots \oplus q_S$.

$$\underbrace{(q_s^\alpha - q_s)}_{\in I^3} \otimes \underbrace{(\phi_s - n_s)}_{\in I} \in I^4$$

$$i_3(\rho_1 \oplus \rho_2) = i_3(\rho_1) + i_3(\rho_2)$$

$$i_3(\rho_1 \otimes \rho_2) = i_3(\rho_1)\,\mathrm{rang}(\rho_2) + i_3(\rho_2)\,\mathrm{rang}(\rho_1)$$

α fixé

$$i_3(\alpha) : R(G) \longrightarrow H^3(K).$$

déterminé par ses valeurs sur des générateurs de $R(G)$, par exemple sur les représentations "fondamentales" $\rho_1, \dots, \rho_\ell$ correspondant aux poids fondamentaux $\omega_1, \dots, \omega_\ell$.

Le cas de G_2

$G = G_2$ déployé

$\alpha \in H^1(K, G_2)$, d'où G_α tordu

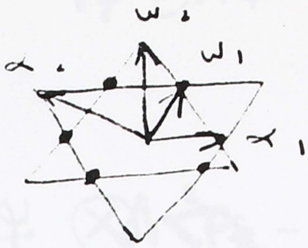
C_α algèbre d'octonions

forme norme φ_α (3-forme de Pfister)

Inversement, toute 3-forme de Pfister définit un α et un seul. On a :

$i_3(\varphi_\alpha) \in H^3(K)$.

Deux représentations fondamentales.

Poids et racines : 

① $\underline{\text{dim } 7}$ poids 0 et les 6 racines courtes

Trace 0 dans alg. d'octonions

Forme quadratique : la norme $N = \varphi$.

déployé, [illegible]

$$\varphi \simeq <1, \underbrace{\alpha, \beta, \gamma, \alpha\beta, \alpha\gamma, \beta\gamma, \alpha\beta\gamma}_{\varphi_7}>$$

$$\varphi \simeq <1> \oplus \varphi_7$$

Forme quadratique : la norme $N = \varphi$ sur les éléments de trace 0, i.e. φ_7.

$$\varphi_7^\alpha - \varphi_7 = \varphi^\alpha - \varphi \qquad (\varphi^\alpha = <1> \oplus \varphi_7^\alpha)$$

Donc le i associé à cette repr. est celui que l'on connaissait déjà.

② $\underline{\text{dim } 14}$

représentation $\underline{\text{adjointe}}$: 2 fois 0, 12 racines.

Forme quadratique : forme de Killing.

$Kill^\alpha$ = forme de Killing de G_α.

Théorème :

$$Kill_\alpha \simeq \langle -1, -3 \rangle \otimes \varphi_7^\alpha .$$

On peut vérifier le cas déployé

$$\mathfrak{g} = \underline{h} \oplus (\text{orthogonal})$$

$$\begin{array}{c} \underbrace{X_\alpha \;,\; X_{-\alpha}} \\ \text{hyperbolique} \end{array}$$

$$\downarrow$$

$$\langle 1, 3 \rangle \quad \simeq x^2 + xy + y^2 .$$

$$\varphi_7 \simeq -1 \quad \text{dans} \quad W(K)$$

D'où le thm dans le cas déployé.

[En caract. 3, cette forme est dégénérée.
La repr. de dim 14 est réductible en car. 3 : somme de 2 repr. de dim 7.]

λ – structure : puissances extérieures

$q \mapsto \Lambda^i q$. défini sur GrW.

$$\Lambda^2 \rho_7 \simeq \rho_7 \oplus \rho_{14}.$$

(dim $21 = 7 + 14$)

$$\rho_{14} \longrightarrow \Lambda^2 \rho_7 \qquad \mathfrak{g} \to SO(V)$$

$$\qquad\qquad\qquad\qquad\qquad \wr\wr$$

$$\qquad\qquad\qquad\qquad\qquad \Lambda^2 V$$

$$\Lambda^2 \rho_7 \longrightarrow \rho_7$$

$x \wedge y \mapsto \pi(xy - yx)$ sur élé. de trace 0.

en fait, $\pi(xy)$ suffit.

On a $\Lambda^2 \rho_7 \simeq \rho_7 \oplus \rho_{14}$. D'où :

$$\begin{array}{cc} \rho_7 & \rho_{14} \\ \downarrow & \downarrow \\ \varphi_7 & \mathrm{Kill} \end{array}$$

$$\Lambda^2 \varphi_7 \simeq \lambda \varphi_7 + \mu \, \mathrm{Kill} \qquad \lambda, \mu \in \mathbb{Q}^\times$$

indép. des choix.

$$\varphi_7 \simeq \langle \alpha, \beta, \gamma, \cdots \rangle$$

$$\lambda^2 \varphi_7 \simeq \langle \alpha\beta, \alpha\gamma, \cdots \rangle.$$

21 produits

On constate que :

$$\lambda^2 \varphi_7 \simeq \varphi_7 \oplus \varphi_7 \oplus \varphi_7$$

Plus généralement : Si φ est une n-forme de Pfister, ~~.....~~ et si on pose :

$\psi = \varphi - \langle 1 \rangle$, alors $\lambda^2 \psi \simeq (2^{n-1} - 1) \otimes \psi.$)

$$\langle 1,1,1\rangle \otimes \varphi_7 \simeq \lambda \varphi_7 + \mu \, \mathrm{Kill}$$

<u>disc</u>. Kill $= 3$ car vrai cas déployé

disc $\varphi_7 = 1$

On trouve $\lambda = 3$ (à un carré près)

$$\langle 3\rangle \varphi_7$$

Calcul de $\mu = ?$ $\quad j : \mathrm{Kill} \hookrightarrow \Lambda^2 \varphi_7$

$$\parallel$$

$$\underline{O} \text{ (7 variables)}$$

Sur l'alg. de Lie d'un groupe orth.

on a la forme trace $\mathrm{Tr}(xy)$. Et :

Kill $=$ 4. forme trace

(dans le cas déployé se voit sur les poids)

$\mathrm{Lie}(\underline{SO}) \simeq \Lambda^2 V$ $\quad$ On a $\begin{cases} \text{Trace} \\ \Lambda^2 q \end{cases}$

Trace : $- 2 \times \Lambda^2 q$

<u>Isom</u> $\underline{SO} \simeq \Lambda^2 V$ donné par

V ev. avec forme bilin. sym.

$$\Lambda^2 V \to \underline{SO}(V)$$

$$v_1 \wedge v_2 \mapsto (x \mapsto B(v_1,x)v_2 - B(v_2,x)v_1)$$

D'où : $\mu = -2$

D'où $\langle -2\rangle \mathrm{Kill} \oplus \langle 3\cancel{\rangle}\varphi_1 \cong \langle 1,1,1\rangle \otimes \varphi_7$

$\cong \langle \cancel{3},2,6\rangle \otimes \varphi_7$

$\langle 1,1,1\rangle = \langle 3,2,6\rangle$

Res K

$\mathrm{Kill} \simeq \langle -1,-3\rangle \otimes \varphi_7$

$\mathrm{Kill}^\alpha \cong \langle -1,-3\rangle \otimes \varphi_7^\alpha$

$\mathrm{Kill}^\alpha - \mathrm{Kill} \cong \langle -1\rangle \otimes \underbrace{\langle 1,3\rangle}_{\in I} \otimes \underbrace{(\varphi_7^\alpha - \varphi_7)}_{\in I^3}$

$(\varphi = \varphi_5)$ $\qquad (\varphi^\alpha - \varphi)$

C'est dans I^4. D'où:

$i_4(\alpha) \in H^4(K)$

$i_4(\alpha) = (-3)\, i_3(\alpha) \in H^4(K)$

$i_3(\alpha, \rho_{14}) = 0.$

Conséquence.

Pour toute représentation φ de G_2, on a soit $i_3(\rho,\alpha) = 0$, soit

$i_3(\rho,\alpha) = i(\alpha) \in H^3(K)$

Si $w = n_1 \varpi_1 + n_2 \varpi_2$, comment calculer explicitement $i_3(\rho,\alpha)$? (Voir p. 111 bis.)

Pour cela, il faut écrire V_w comme polynôme en ρ_1 et ρ_2.

Compléments sur les octonions et sur G_2 :

(1) Bourbaki, alg. III, dernier exercice (faute d'impression !) donne une formule montrant que les sommes de 16 carrés sont multiplicatives) :

C alg. d'octonions $\quad N(x) = x_0^2 + \alpha x_1^2 + \beta x_2^2 + \gamma x$
$\qquad + \alpha\beta x_4^2 + \dots$

Posons : $N(x) + \delta N(y) = \Phi$.

C'est une forme à 16 variables, 4-forme de Pfister.

Formule :

$$(N(x) + \delta N(y)) \cdot (N(z) + \delta N(t)) = N(x\bar{z} + \delta y \bar{t}) + \delta N(xt - xz.x^{-1}$$

$x, y, z, t \in C$

$x^{-1} = \bar{x}/N(x)$.

(2) A-t-on $i_3(\alpha) = 0$ pour tout α (et tt ρ)
(Probablement non.)

Pour F_4, l'invariant $i_3(\rho, \alpha)$ est $\neq 0$ pour certains ρ, α
(par exemple, $K = \mathbb{R}$, ρ repr. adjointe)
forme de Killing, signature

$i_3 \in H^3(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$. Il y a 3 possibilités :

-52 | compacte $\qquad n_+ - n_-$
4 | déployée
-20

F_4 repr. fond. en dim. 26

J Alg. de Jordan except. de dim 27

repr. fond. = élém. de trace 0 dans J.

$\mathrm{Aut}\, J = F_4$

Forme $\mathrm{Tr}(xy)$ sur J, de rang 27

Algèbre de Jordan "réduite" :

$\exists\, e \in J,\ e^2 = e,\ e \neq 0, 1.$

Les J réduites sont définies, au moyen d'une algèbre de Cayley $\mathbb{O}$, et d'une forme hermitienne à 3 variables sur $\mathbb{O}$ → 3 scalaires, $\gamma_1, \gamma_2, \gamma_3 \in K^*$. Autrement dit, J est formée des matrices 3×3, à coeff. ds $\mathbb{O}$, hermitiennes par. rap. $\begin{pmatrix} \gamma_1 & & 0 \\ & \gamma_2 & \\ 0 & & \gamma_3 \end{pmatrix} = \Gamma$ $\quad (A\Gamma = \Gamma\, {}^t\bar{A})$

$$J = \begin{pmatrix} x_1 & c_3 & c_2 \\ \lambda_3 \bar{c}_3 & x_2 & c_1 \\ \lambda_2 \bar{c}_2 & \lambda_1 \bar{c}_1 & x_3 \end{pmatrix}$$

où $x_i \in K$, $c_i \in C$

et $\lambda_1 = \gamma_3/\gamma_2$, $\lambda_2 = \gamma_3/\gamma_1$, $\lambda_3 = \gamma_2/\gamma_1$

$H^1(K, F_4)_{\mathrm{red}} \subset H^1(K, F_4)$

$\shortparallel$

classes de J (réduites)

J détermine l'algèbre d'octonions O

3 - forme de Pfister q_8

5 - forme de Pfister $q_{32} = q_8 \otimes \varphi_4$, où

$\varphi_4 = \langle 1, \gamma_1^{-1}\gamma_2, \gamma_2^{-1}\gamma_3, \gamma_3^{-1}\gamma_1 \rangle$.

J est déterminé à isom. près par φ_8, φ_{32} que l'on peut se donner arbitrairement

En effet, $\underset{q_8}{\overset{\varphi_8}{\shortparallel}}$ et $\varphi_{32} \Longleftrightarrow$ forme trace de J

(Springer)

Conj. de Milnor $\Rightarrow$ les alg. de Jordan réduites sont définies par

$$\left[\begin{array}{l} x_3 \in H^3(K) \\ x_5 \in H^5(K) \end{array}\right.$$ avec les conditions

① x_3 est décomposable

② $x_5 \in x_3 \cdot H^2(K)_{dec}$

Exemple : $K = \mathbb{R}$:

$x_3 = 0$, $x_5 = 0 \Rightarrow$ déployé

$x_3 \neq 0$, $x_5 = 0$

$x_3 \neq 0$, $x_5 \neq 0$ (exercice...)

Ce sont les 3 cas de tout à l'heure

La forme trace est $Q_J = 2(x_1^2 + x_2^2 + x_3^2) + \gamma_1^{-1}\gamma_2 N(c_3)$

$+ \text{———} \qquad + \gamma_2^{-1}\gamma_3 N(c_2).$

i.e. $Q_J = \langle 2,2,2\rangle \oplus \langle \gamma_1^{-1}\gamma_2, \gamma_2^{-1}\gamma_3, \gamma_3^{-1}\gamma_2\rangle \otimes N.$

La connaissance de QJ détermine à la fois la 3-forme de Pfister N et la 5-forme de Pfister $N \otimes \langle 1, \gamma_1^{-1}\gamma_2, \dots\rangle$.

On a $N \in I^3$, $\gamma N \in I^3$, $\gamma N \equiv N \mod I^4$

$$Q_J - \langle 2,2,2\rangle \equiv N \mod I^4.$$

Or, si N, N' sont des 3-formes de Pfister, on a

$$N \equiv N' \pmod{I^4} \Rightarrow N \simeq N'.$$

$$5\text{-forme} = Q_J - \langle 2,2,2\rangle \oplus N.$$

———

La forme trace d'une algèbre d'octonions détermine l'algèbre, et est une 3-forme de Pfister. Voici pourquoi :

Soient C, N ; C', N' alg. d'octonions, et formes traces associées.

Supposons $N \simeq N'$.

$N = \langle 1\rangle \oplus \varphi_7$, $N' = \langle 1\rangle \oplus \varphi'_7$

$\varphi_7 \cong \varphi'_7$. On choisit $\alpha \neq 0$ tel que $-\alpha$ est représenté par φ_7 et φ'_7.

D'où $e_1 \in C$, $\operatorname{Tr} e_1 = 0$, $e_1^2 = -\varphi_7(e_1) = \alpha$

et $e_1' \in C'$ ——— $e_1'^2 = \alpha$.

On pose $K_2 = K \oplus K e_1$ et $K_2' = K \oplus K e_1'$.

Sur $K_2^\perp$ on a $\varphi_6 = \varphi - \langle 1, \alpha \rangle$ et de même φ_6'.

Par Witt : $\varphi_6 \cong \varphi_6'$

Il existe (donc) $-\beta \neq 0$ représenté par φ_6, φ_6'.

D'où $\left| \begin{array}{l} e_2 \in C, \quad e_2 \perp (1, e_1), \quad e_2^2 = \beta \\ e_2' \in C' \quad ——— \quad e_2'^2 = \beta. \end{array} \right.$

On pose $K_4 = K_2 \oplus K_2 e_2$ et $K_4' = K_2' \oplus K_2' e_2'$.

La Structure d'algèbre (de K_4) est déterminée par celle de K_2, $e_2^2 = \beta$, $e_2 \perp \langle 1, e_1 \rangle$. (Voir plus loin.)

K_4 de dim. 4

Dans $K_4^\perp$, on choisit $e_3 \in K_4^\perp$, $e_3^2 = \gamma$,

et $e_3' \in K_4'^\perp$, $e_3'^2 = \gamma$.

On a $C = K_4 \oplus K_4 \cdot e_3$

$C' = K_4' \oplus K_4' \cdot e_3'$

On trouve l'alg. d'oct. sur α, β, γ.

Formules de produit : $\quad c, d \in K_4 \quad e_3^2 = \gamma$

$$(a + b e_3)(c + d e_3) = ac + \gamma \bar{d} b + (da - b\bar{c}) e_3 .$$

(Autre façon (Tits) –

V de dim. 8, q de disc. 1
inv. de Witt trivial

V', V'' repr. semi-spinorielles $\qquad V \otimes V'$ fait intervenir V'', etc.

On normalise un système de vecteurs de longueur 1, soit e, e', e''. On identifie V, V', V'' (formes isom.), Loi de produit des oct.

SO_3 opère sur V, V', V''

?

$(x, y) \longmapsto xy)$

$C \cong$ alg. oct)

$(g \in \mathrm{Spin}\ C$.

Retour aux généralités sur les f. q.

théorèmes d'injectivité du H^1

1) Thm de Witt : $\qquad q = q' \oplus q''$

$$O(q') \hookrightarrow O(q)$$

donne $\quad H^1(K, O(q')) \longrightarrow H^1(K, O(q))$

(2) Pfister $\quad q = q' \otimes q''$

$$O(q') \longrightarrow O(q)$$
$$x \longmapsto x \otimes 1$$

Th Si rang q'' est impair, l'application

$$H^1(K, O(q')) \longrightarrow H^1(K, O(q))$$

est injective

(3)

Th (Springer)

Si K'/K est une ext. de degré impair, alors la flèche naturelle

$$H^1(K, O(q)) \longrightarrow H^1(K', O(q)) \text{ est injective}$$
$$\|$$
$$H^1(K, O(q)) \to H^1(K, R_{K'/K}\, O(q))$$

(2) $\Rightarrow$ (3)

(D'abord, énoncés en termes de f.q.)

K'/K extension. f.q. $/K' \to$ f.q. $/K$. On se donne $\lambda : K' \to K$, K-forme linéaire $\neq 0$

ψ f.q. sur V'/K' $\mapsto$ $x \mapsto \lambda(\psi(x))$, f.q. sur V'/K

$\psi \mapsto \psi_\lambda$.

Cas part. $\Psi = x^2$ sur K', $n = [K' : K]$

Ψ_λ forme : $x \in K' \longmapsto \lambda(x^2) = q_{\lambda}(x)$ (n variables).

$$\Psi \simeq \sum_{i=1}^{r} \alpha_i x_i^2 \quad , \quad \alpha_i \in K^*$$

$$\Psi_\lambda \simeq \sum \alpha_i \lambda(x_i^2) \simeq \langle \alpha_1, \dots, \alpha_r \rangle \otimes q_\lambda$$

$$\Psi_\lambda \equiv \Psi \otimes q_\lambda .$$

Autre façon de voir :

$$O(q) \longrightarrow R_{K'/K}\, O(q) \to O(q \otimes q_\lambda)$$

$O(q)$, repr. ρ

Condition générale sur ρ pour obtenir injectivité au niveau des H^1 ? On ne sait pas...

car $K \neq 2$

① Théorème de simplification de Witt

$$H^1(K, O(q)) \longrightarrow H^1(K, O(q+q'))$$

est injectif

② (Arason – Pfister) même énoncé avec $q \otimes q'$, et rang q' impair.

③ (Springer) K'/K de degré impair

$$H^1(K, O(q)) \to H^1(K', O(q))$$

est injectif

$$\| \\ H^1(K, R_{K'/K} O(q))$$

② ⟹ ③ fait

Démonstration de ②

Il suffit de montrer que $q \mapsto q \otimes q'$ définit une injection

$$W_K \longrightarrow W_K .$$

② ⟺ (q') dans W_K est non diviseur de

q' est de rang impair ⟺ $q' \notin I$

$$W_K / I \cong \mathbb{Z}/2\mathbb{Z} \quad (\text{rang})$$

Lemme: $\bigcap I^n = 0$ dans W_K

Supposons que non. Alors il y aurait une f.q. Q anisotrope de rang ≥ 1, t.q.

$(Q) \in I^n$ pour tout n.

Impossible si rang $(Q) < 2^n$.
q' est inversible mod tout I^n.

On voudrait avoir un critère, étant donné

$$\varphi : O(q) \to O(Q)$$

critère pour l'injectivité sur le H^1 ?
Par exemple, puissances extérieures ?

1 On peut supposer q' de rang 1.
$q' = \langle a \rangle$, $a \in K^*$.
Il suffit de démontrer que le noyau est 0.

$G_1 \subset G_2$ groupes algébriques

Ker : $H^1(K, G_1) \to H^1(K, G_2) = ?$

$$1 \to H^0(G_1) \to H^0(G_2) \to H^0(\underbrace{G_2/G_1}_{X}) \to$$

$$\to H^1(G_1) \to H^1(G_2)$$

Le noyau est donc

$X(K)/G_2(K)$: ensemble des orbites de $G_2(K)$ dans $X(K)$.

Injectivité $\Longleftrightarrow$ $G_2(K)$ opère transitivement sur les points rationels de l'espace homogène $X = G_2/G_1$.

Ici $X = O(\overbrace{q+q'}^{Q})/O(q)$

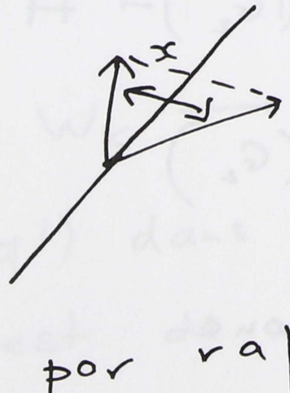
O_{n+1}/O_n

$\wr\wr$

Sphère des $x \in K^{n+1}$ avec $Q(x) = a$.

Quadrique affine. On est donc ramené à prouver l'énoncé classique suivant :

(1') (Witt) Si x, y sont deux vecteurs tels que $Q(x) = Q(y)$ $(\neq 0)$ alors il existe $s \in O(Q)$, rat./K, qui transforme x en y.



réflexion par rapport à $x-y$ si $x-y$ anisotrope. Si $x+y$ non isotrope, réflexion par rapport à $x+y$.

$x-y$, $x+y$ tous les deux isotropes est impossible (sinon $x \cdot x = 0$).

2 et 3 :

$$O_n \hookrightarrow O_{nm} \quad m \text{ impair}$$

montrer directement que l'action de $SO_{nm}(K)$ sur les points rationnels de O_{nm}/O_n est transitive ??

3 (Springer) 2 variantes de démonstration

a) démonstration de Scharlau

$\lambda : K' \to K$ forme linéaire non nulle

$n = [K' : K]$ $\quad \lambda \mapsto q_\lambda$ de rang n

$$q_\lambda(x) = \lambda(x^2).$$

$$W_K \xrightarrow{i} W_{K'} \xrightarrow{\lambda} W_\lambda$$

$$\lambda \circ i(q) = q \otimes q_\lambda$$

Il existe des choix de λ qui sont tels que $(q_\lambda) \simeq \langle 1 \rangle$ dans W_K.

Choix de λ :

Supposons d'abord que K' soit une extension monogène de K. Soit $t \in K'$ tel que $K' = K(t)$

K' base $1, t, \ldots, t^{n-1}$.

$\lambda(1) = 1 \qquad \lambda(t^i) = 0 \quad , \ 1 \leq i \leq n-1.$

Lemme — $q_\lambda \cong \langle 1 \rangle \oplus \frac{n-1}{2} \cdot$ forme hyperbolique

$$K' = K \oplus V, \quad V = Kt \oplus \cdots \oplus Kt^{n-1}$$

$$q_\lambda(x,y) = \lambda(x \cdot y)$$

$$q_\lambda = \langle 1 \rangle \oplus q_{\lambda,V}$$

V contient $W = Kt \oplus \cdots \oplus Kt^{\frac{n-1}{2}}$

$W \cdot W \subset V, \quad \lambda(w \cdot w) = 0$

donc W est totalement isotrope de dimension $\frac{n-1}{2} \Rightarrow q_{\lambda,V}$ est hyperbolique.

D'où le lemme : on a bien $q_\lambda \simeq \langle 1 \rangle$ dans W_K.

Cas général : récurrence sur le degré de K

$$K' \supset K'' \supset K \qquad \lambda = \lambda'' \circ \lambda'.$$

$$K' \xrightarrow{\lambda'} K'' \xrightarrow{\lambda''} K$$

b) Méthode de Springer

Théorème (Springer)

Soit K'/K de degré impair. Soit q une forme quadratique sur K. Si q représente 0 sur K', q représente 0 sur K.

Ou encore :

q anisotrope sur K $\Rightarrow$ q anisotrope sur K'.

Entraîne l'énoncé précédent.

Vrai en carac 2 aussi, avec la même démonstration.

Démonstration :

On peut supposer K'/K monogène,

$K' = K[t]/(p(t))$ $\quad p$ unitaire, irréductible de degré n

Récurrence sur n.

$x = (x_1, \dots, x_N)$ $\quad N$ variables.

$q(x'_1, \dots, x'_N) = 0$ $\quad x'_i \in K'$ non tous nuls.

$x'_i = \alpha_i(t)$ $\quad d^\circ \alpha_i \leq n-1$, α_i sans facteur commun

$Q = q(\alpha_1(t), \dots, \alpha_N(t)) \equiv 0 \mod p(t)$

$Q(t)$ de degré ?

Soit r le maximum des degrés des α_i.

$\alpha_i = \lambda_i t^r + \dots + \dots$ avec λ_i non tous nuls.

$$Q = q(\alpha_1 t^r + \cdots, \alpha_2 t^r + \cdots, \ldots, \alpha_N t^r + \cdots)$$

$$= t^{2r} q(\alpha_1, \ldots, \alpha_N) + \text{polynôme de degré au plus } 2r-1$$

q est anisotrope : $q(\alpha_1, \ldots, \alpha_N) \neq 0$.

Donc degré de $Q = 2r \leq 2n-2$

$Q = p\, Q'$ $\quad$ $\deg Q' = 2r - n$

$\leq n-2$.

impair

Soit p' un facteur irréductible de degré impair de Q'.

$Q \equiv 0 \pmod{p'}$

$a_i(t)$ ne sont pas tous $0 \bmod p'$.

Donc Q représente 0 dans le corps $K(t)/(p')$

Contradiction, car $K(t)/(p')$ est de degré $\leq n-2$.

Démonstration constructive.

Corollaires du théorème de Springer

$[K':K]$ impair.

1 Soient q_1, q_2 deux formes quadratiques sur K de rang r_1, r_2, $r_1 \geq r_2$.

Supposons que q_1 contienne q_2 sur K' alors q_1 contient q_2 sur K.

"contient" : $q_1 \cong q_2 \oplus q_3$.

(*) q_1 contient q_2 $\Longleftrightarrow$ $q_1 \oplus (-q_2)$ contient r_2 fois la forme $h = \langle 1, -1 \rangle$

$\Rightarrow$

$q_1 = q_2 \oplus q_3$ $\quad q_1 \oplus (-q_2) = q_2 \oplus (-q_2) \oplus q_3$

$\langle a \rangle \oplus \langle -a \rangle \cong \langle 1, -1 \rangle$.

$\cong r_2 h \oplus q_3$

$\Leftarrow$

$q_1 \oplus - q_2 = r_2 h \oplus q_3$

$= q_2 \oplus (-q_2) \oplus q_3$

$\Rightarrow q_1 \cong q_2 \oplus q_3$ par Witt.

On est donc ramenés à prouver que si q contient m fois h sur K', q contient m fois h sur K.

$$Q = Q_{anis} + x\,h \qquad x \geq m \quad /K'$$

$$x \geq m \quad /K$$

(2) q forme quadratique $/K$

<u>Si</u> q <u>est une</u> n- <u>forme de Pfister</u> sur K'

<u>alors</u> — " — <u>sur</u> K

rang $q = 2^n = N$

q n-forme de Pfister $\Longleftrightarrow$ q est hyperbolique ou q anisotrope et il existe $z_1, \dots, z_N \in K(X, Y)$ telles que
$$q(X)\,q(Y) = q(Z).$$

ou bien q est hyperbolique $/K'$ donc sur K

ou bien des $z_i' \in K'(X,Y)$ existent avec
$$q(X)\,q(Y) = q(Z').$$

q représente $q(X)\,q(Y)$ sur $K'(X,Y) = K' \otimes_K K(X,Y)$ de degré impair sur $K(X,Y)$

$q(x)q(y) \in K(x,y)$ est représenté

sur $K'(x,y)$, donc sur $K(x,y)$

$m = 1, 2, 3, 4$

q m-forme de Pfister $\iff$ q représente

$H^i(K) \to H^i(K')$ injectif.

invariants de q dans $H^1, H^2, \ldots H^{m-1}$ sont 0

Questions.

$W_K \to W_{K'}$ est injectif

$$\begin{array}{ccc} k_m^M K & \longrightarrow & I_K^m / I_K^{m+1} \\ & \searrow & \\ & & H^m(K) \end{array}$$

conj : isom.

on passe à K' $\leadsto$ diagramme

$H^m(K) \longrightarrow H^m(K')$ injectif

(a) $k_n^M K \to k_n^M K'$ injectif ?

$\boxed{\text{oui}}$: Bass-Tate, Kato

(trace) LN 342, p. 379, corollary

(b) $I^m_K / I^{m+1}_K \to I^m_{K'} / I^{m+1}_{K'}$

injectif

Oui : car le transfert $I^m_{K'} \to I^m_K$

J.K.

(Arason) Cohomologische Invarianten Quadratischen Formen, J. of Algebra 36 (1975), p. 448-491, p. 464, Satz 3.3.

voir aussi les 2 lignes du haut de la p. 465

Formes trace ; cas des algèbres centrales simples.

car $K \neq 2$

A algèbre simple centrale sur K

de rang n^2

$[A] \in Br(K)$

Trd = trace réduite de A

$q_A(x) = Trd(x^2)$

forme bilinéaire correspondante ($= \frac{1}{2}$ associée)

est $Trd(xy)$

cas déployé : $A = M_n(K)$

$Trd(x) = Tr(x)$ $x \in M_n(K)$, $x = (x_{ij})$

$$Tr(x^2) = \sum x_{ii}^2 + 2 \sum_{i<j} x_{ij} x_{ji} \text{ . D'où :}$$

$$q_A^{dec} = \underbrace{\langle 1, \dots, 1 \rangle}_{n} + \frac{n(n-1)}{2} h \qquad h = \langle 1, -1 \rangle.$$

On va comparer q_A et q_A^{dec}.

1er cas : n impair

Alors $q_A \cong q_A^{dec}$

En effet, il existe K'/K de degré impair qui décompose A.

Donc $(*)$ est vraie sur K' $\Rightarrow$ vraie sur K (grâce au théorème de Springer). Voici une application :

Thm (Wedderburn): car $K \neq 3$

Si $n=3$, A est une algèbre cyclique.

$[A] \in Br_3(K)$ peut s'écrire

$[A] = x \cdot y$, $x \in H^1(K, \mu_3)$
$y \in H^1(K, \mathbb{Z}/3\mathbb{Z})$

$\Updownarrow$

A contient un corps cubique cyclique

car $K \neq 2, 3$

A montrer : il existe $\alpha \in A$ avec

$\alpha^3 \in K^*$ et $Trd(\alpha) = 0$, $Trd(\alpha^2) = 0$.

pol. caract. $t^3 - x$

Soit V espace vect. de dim 8, $Trd(\alpha) = 0$.

$q_A | V$ forme de rang 8

$q_A | V$ représente 0. Sinon,

q_A = anisotrope de rg 8 $\oplus \langle \lambda \rangle$.

Si K contient μ_3, $A \supset K(\alpha) = K(\sqrt[3]{x})$

Si $\mu_3 \notin K$, posons $L = K(\mu_3)$.

On a une involution $z \mapsto \bar{z}$ de L

opère sur la cohomologie de L.

On dispose d'un $x \in K^*$, non cube, tel que

$K(\sqrt[3]{x}) \subset A$, d'où $L(\sqrt[3]{x}) \subset A_L$.

Donc, dans $H^2(L, \mu_3)$, $[A] = x \cdot y$

avec $y \in H^1(L, \mathbb{Z}/3\mathbb{Z})$.

$H^1(K, \mathbb{Z}/3\mathbb{Z})$

(resp. μ_3) $\overset{\downarrow}{=}$ points fixes de l'involution

agissant sur:

$H^1(L, \mathbb{Z}/3\mathbb{Z})$,

[resp. $H^1(L, \mu_3)$];

même chose pour: $H^2(L, \mu_3)$.

On écrit $y = y^+ \oplus y^-$, avec

y^+ invariant

y^- anti-invariant.

$[A] = xy^+ + xy^-$; (invariant) $[A] = [A^+]$

$x = x^+$

$[A] = xy^+$

donc : $y^+ \in H^1(K, \mathbb{Z}/3\mathbb{Z})$, et l'on a

$[A] = xy^+$, cqfd.

En fait, pour p premier et A algèbre centrale simple de rang p^2, A est cyclique $\Longleftrightarrow$ A^* contient a, $a \notin K$,

$a^p \in K$

autrement dit, $A \supset K(\sqrt[p]{x})$

$x \in K^*$.

<u>Remarque</u> –

$p = 3$ $\quad a^3 \in K^*$, $a \notin K$

$x \mapsto axa^{-1}$ automorphisme de A d'ordre 3.

Suffisant de ~~prouver~~ trouver un sous-corps L commutatif maximal de A, stable par σ, mais pas fixé par σ.

PGL(A) groupe alg. plusieurs tores maximaux stables, ??

cas 2 :

à résoudre $\mathrm{Tr}\, a = 0$, $\mathrm{Tr}\, a^2 = (\mathrm{Tr}\, a)^2 = 0$

sol. après ext. de degré impair

$\rightarrow$ solution.

cas 3 : facile.

Le cas pair

n pair, $q_A = ?$ A de degré n^2.

Structure complète pas connue, mais on va donner plusieurs renseignements.

Théorème $\quad w_1(q_A) = w_1(q_A^{dec}) = n_2(-1) \in H^1(K)$

$$q_A^{dec} = n\langle 1\rangle \oplus n_2 h \qquad \text{où } h = \langle 1, -1\rangle$$

et $n_2 = \dfrac{n(n-1)}{2}$.

Théorème $\quad w_2(q_A) = w_2(q_A^{dec}) + \frac{n}{2}[A]$.

$[A] \in Br_n(K)$ et $n[A] = 0$, d'où

$\frac{n}{2}[A] \in Br_2(K)$.

$A = (A^{dec})_\alpha$, $\alpha \in H^1(K, PGL_n)$

$A^{dec} = M_n$

$PGL_n = \mathrm{Aut}(A^{dec})$

A^{dec} est un espace vect. muni de la forme quadratique q_A^{dec} $(Tr(xy))$

Tout automorphisme de A^{dec} respecte q_A^{dec}

(n^2 var.)

$$PGL_n \xrightarrow{\varphi} O(q_A^{dec})$$

$$\| $$

$$\mathrm{Aut}(A^{dec})$$

$$H^1(K, PGL_n) \xrightarrow{\psi} H^1(K, O(q_A^{dec}))$$

$(\psi = H^1(\varphi))$

Foncteur algèbe simple centrale → espace quadr.

q_A est la tordue de q_A^{dec} par

$\psi\alpha \in H^1(K, O(q^{dec}))$

$$\delta^1 : H^1(K, O(q)) \longrightarrow H^1(K, \mathbb{Z}/2\mathbb{Z})$$

$$1 \longrightarrow SO(q) \to O(q) \longrightarrow \{\pm 1\} \to 1$$

$$w_1(q_\beta) = w_1(q) + \delta^1(\beta) \qquad \beta = \psi\alpha$$

Par connexité, l'image de PGL_n ds $O(q^{dec})$ est contenue dans $SO(q^{dec}) \Rightarrow \delta^1\beta = 0$.

$$\begin{array}{c} 1 \\ \downarrow \\ \pm 1 \\ \downarrow \\ \mathrm{Spin}(q) \\ \downarrow \\ SO(q) \\ \downarrow \\ 1 \end{array}$$

$$\delta^2 : H^1(SO(q)) \longrightarrow H^2(K, \mathbb{Z}/2\mathbb{Z})$$

$$w_2(q_\beta) = w_2(q) + \delta^2(\beta)$$

$$\beta \in H^1(K, SO(q))$$

$$\begin{tikzcd} \mu_n \arrow[r] \arrow[d] & \mu_2 \arrow[d] \\ SL_n \arrow[r, "\nu"] \arrow[d] & \mathrm{Spin}(q_A^{dec}) \arrow[d] \\ PGL_n \arrow[r, "\varphi"] & SO(q_A^{dec}) \end{tikzcd}$$

car SL_n est simplement connexe.

$$\nu(\zeta) = \begin{cases} 1 \\ \zeta^{n/2} \end{cases}$$

$$\nu(\zeta) = \zeta^{n/2}$$

<u>Lemme</u> :

Donc ν est surjectif.

admettons le lemme pour le moment.

$$\begin{array}{ccc} \alpha \in H^1(K, PGL_n) & \to & H^2(K, \mu_n) = Br_n(K) \\ \downarrow \gamma & & \downarrow \\ H^1(K, SO) & \longrightarrow & H^2(K, \mu_2) \end{array}$$

L'image de α ds $Br_n(K)$ est $-[A]$

$\frac{n}{2}(-[A]) = \frac{n}{2}[A]$.

D'où $\delta^2(\beta) = \frac{n}{2}[A]$

et la formule en résulte.

[Si car divise n, il faut prendre la cohomologie plate.]

Il reste à prouver le lemme :

si γ non surjectif, $\gamma = 1$,

la flèche $SL_n \to Spin$ $\tilde{\varphi}$

se factoriserait en $PGL_n \to Spin$

φ se relèverait en $\tilde{\varphi}$.

$$\begin{array}{ccc} & & Spin_{n^2} \\ & \nearrow & \downarrow \\ PGL_n & \to & SO_{n^2} \end{array}$$

à voir que non.

Technique connue en th. des groupes alg. pour voir si une repr. se relève aux spineurs.

G réductif connexe, φ représentation orthogonale de G.

On choisit un tore maximal T.

Poids de ρ (écrits additivement)

poids 0 multiplicité quelconque

paires $(w_i, -w_i)_{i\in I}$ avec même multiplicité, $w_i \neq 0$.

On forme alors $\sum_{i\in I} w_i$; le critère est :

$$\sum w_i \equiv 0 \pmod 2 \text{ dans } X(T)$$

(les w_i sont répétés suivant leurs multiplicités)

$$\Updownarrow$$

ρ spinorielle

(remarquons que $-\frac{w_1}{2} + \cdots + \frac{w_n}{2} = \frac{w_1}{2} + \cdots + \frac{w_n}{2} - w_1$)

Ici, on a :

$GL_n \to PGL_n$ $\quad e_1, \ldots, e_n$ poids de repr. évidente de GL_n.

Groupe des poids de PGL_n est l'ens. des $m_1 e_1 + \cdots + m_n e_n$ avec $m_i \in \mathbb{Z}$ et $m_1 + \cdots + m_n = 0$

(il est engendré par les $e_i - e_j$).

Les poids de PGL_n agissant sur M_n par autom. int. soient les $e_i - e_j$ $\quad i, j \in [1, n]$.

Les non nuls sont les $e_i - e_j$ $(i<j)$

et leurs opposés (mult. 1)

On forme $\omega = \sum_{i<j} (e_i - e_j)$ div par 2 dans les poids de PGL_n ?

non !

coeff de e_1 dans $\sum_{i<j} (e_i - e_j)$

$= n-1$ impair.

$\omega = (n-1)e_1 + \cdots$ $\omega \neq 0 \pmod 2$ car n est pair.

4 mars 1991

Rappel sur G_2

<u>car 0</u> $\quad i : H^1(K, G_2) \hookrightarrow H^3(K, \mathbb{Z}/2\mathbb{Z})$

$\omega = n_1 \omega_1 + n_2 \omega_2$

repr. $\rho_\omega : H^1(K, G_2) \longrightarrow H^1(K, SO_\omega)_{spin} \to H^3(K)$

$i_\omega : H^1(K, G_2) \longrightarrow H^3(K)$

$i_\omega = \begin{cases} 0 & \omega = 0 \text{ unité ou } \omega = \omega_2 \text{ (dim 14)} \\ \text{ou} & \\ i & \omega = \omega_1 \text{ (repr. de dim 7)} \end{cases}$

$\omega \equiv \omega' \pmod 8 \implies i_\omega = i_{\omega'}$.

Pour $n_1, n_2 \leq 8$, on détermine les valeurs de i_ω (voir tableau, page suivante)

<u>retour à $Tr(x^2)$</u>

A algèbre simple centrale, $n^2 = [A:K]$

$q_A(x) = Trd(x^2)$ $\quad$ rang n^2

n impair $\quad q_A \simeq q_A^{dec}$

n pair $\quad w_1(q_A) = w_1(q_A^{dec})$

$\quad w_2(q_A) = w_2(q_A^{dec}) + \frac{n}{2}[A]$

$q_A - q_A^{dec} \in I_K^2 \qquad I_K = \text{idéal max. de } W_K$

$cl(q_A - q_A^{dec}) \in I_K^2 / I_K^3 \cong Br_2(K)$

$\qquad\qquad \overset{\shortparallel}{\frac{n}{2}[A]}$.

Tableau donnant les valeurs de l'invariant i_ω pour G_2

—

On écrit $\omega = n_1\omega_1 + n_2\omega_2$ où ω_1, ω_2 sont les 2 poids fondamentaux ($\omega_1 \to$ repr. de dim. 7 ; $\omega_2 \to$ rep. adjointe).

L'invariant i_ω est $\varepsilon_\omega i$, avec $\varepsilon_\omega = 0$ ou 1, i étant l'invariant naturel ($= i_{\omega_1}$).

La valeur de ε_ω ne dépend que de $n_1, n_2 \pmod 8$. Elle est donnée par le tableau suivant (en caract. 0)

Valeur de $\varepsilon_\omega \to$

$n_1 \backslash n_2$	0	1	2	3	4	5	6	7
0	0_{1}	0_{14}	1_{77}	1_{273}	0	0	0	0
1	1_{7}	0_{64}	0_{286}	0	1	0	0	0
2	1_{27}	0_{189}	0	1	0	0	0	0
3	0_{77}	0	0	0	0	0	0	0
4	0_{182}	0	0	1	0	0	1	0
5	0	0	1	0	0	0	1	0
6	0	0	0	1	1	0	0	0
7	0	0	0	0	0	0	0	0

(En indice : dimension de la rep., en car. 0)

Noter $i_\omega = 0$ si $n_2 \equiv 1, 5, 7 \pmod 8$

Cas particulier $n = 4$

$[A] \in Br_4(K)$, $\frac{n}{2}[A] = 0$: $[A] \in Br_2(k)$

Alors $A = A_1 \otimes A_2$, A_λ alg. quat.

$A_\lambda = (a_\lambda, b_\lambda)$ $\lambda = 1, 2$.

$q_A - q_A^{dec} \in I_K^3$. Image ds $I_K^3 / I_K^4 \simeq H^3(K)$

$q_A = q_{A_1} \otimes q_{A_2}$.

Soit (a, b) un corps de quaternions.

Forme norme N:

$x = x_0 + x_1 i + x_2 j + x_3 k$, $k = ij$

$Nx = x_0^2 - a x_1^2 - b x_2^2 + ab x_3^2$

$N_{(ab)} = \langle 1, -a, -b, ab \rangle$.

Forme trace:

$x^2 = (x_0^2 + a x_1^2 + b x_2^2 - ab x_3^2) + \cdots$

$q_{(a,b)} = 2 \langle 1, a, b, -ab \rangle$

$q_A = \langle 1, a_1, b_1, -a_1 b_1 \rangle \otimes \langle 1, a_2, b_2, -a_2 b_2 \rangle$

comparer à la norme:

$N_{ab} + \langle \frac{1}{2} \rangle q_{(a,b)} = \langle 1 \rangle + \langle 1 \rangle = 2$

dans W_K

$q_A = (2 - N_1) \otimes (2 - N_2)$ $N_1 = N_{a_1, b_1}$, $N_2 = N_{a_2, b_2}$.

$N_\lambda = N_{a_\lambda, b_\lambda}$. $\quad q_A^{dec} = 4$.

$$q_A - q_A^{dec} = 4 - 2(N_1 + N_2) + N_1 N_2 - 4$$
$$= -2(N_1 + N_2) + N_1 N_2 .$$

$2 \in I_K$, $\quad N_\lambda \in I_K^2$, donc

$$q_A - q_A^{dec} \in I_K^3 .$$

Classe dans I_K^3 / I_K^4 ?

$$2 \longrightarrow I_K / I_K^2 = H^1(K)$$

$\overset{\shortparallel}{\langle 1 \rangle - \langle -1 \rangle}$

$$2 \longrightarrow (-1) \in H^1(K) .$$

$$q_A - q_A^{dec} \longrightarrow (-1)(x_1 + x_2) = (-1)[A] \in H^3(K).$$

$x_\lambda = [A_\lambda] \in H^2(K)$

Que se passe-t-il si -1 est un carré ds K ?

$(-1) = 0$ ds $H^1(K)$.

$2 = \langle 1 \rangle - \langle -1 \rangle = 0$ $\quad$ (car $\langle 1 \rangle = \langle -1 \rangle$)

$2 = 0$ dans W_K.

$q_A - q_A^{dec} = N_1 \cdot N_2 \in I_K^4$

Classe de $q_A - q_A^{dec}$ dans I_K^4 / I_K^5

est le cup-produit $x_1 \cdot x_2$, où $x_\lambda = [A_\lambda] \in H^2(K)$.

$x = [A]$, $x = x_1 + x_2$. $x_\lambda = (a_\lambda)(b_\lambda)$

$\longmapsto x_1 x_2 \in H^4(K)$.

ce produit ne dépend pas de la décomposition

$x = x_1 + x_2$.

Suggère chercher une opération cohomologique:

$$-1 = \square$$

Théorème: (Sous l'hypothèse que -1 est un carré dans K.)

Il existe une unique application

$$\varphi : H^2(K) \to H^4(K)$$ telle que:

ⓐ $\varphi(x+y) = \varphi(x) + \varphi(y) + xy$

ⓑ $\varphi(x) = 0$ si $x = a \cdot b$, avec $a, b \in H^1(K)$.

Si on admet ce thm, $\varphi(x) = x_1 x_2$ est l'application ci-dessus.

Cartan a étudié la notion de

Puissance divisée dans les algèbres. $\left(\frac{x^n}{n!}\right)$

C anneau commutatif, J idéal

$\gamma_i : J \to C$ $\quad i = 0, 1, 2, \dots$

$\gamma_0(x) = 1$, $\gamma_1(x) = x$, ... $\gamma_n(x+y) = \sum_{i+j=n} \gamma_i(x)\gamma_j(y)$

(d'autres propr.) $\quad \gamma_n(xy) = x^n \gamma_n(y)$ $\quad y \in J$, $x \in C$

(dans Cartan : C commutatif gradué, J : idéal des élé de degré ≥ 1)

$\Rightarrow n!\,\gamma_n(x) = x^n$.

<u>Exemple</u> : k anneau commutatif

M k-module

$$C = \Lambda^{\text{pair}} M$$

Il y a sur C (sur les élé > 0)

des γ_i uniques tels que

$$\gamma_i(x_1 \wedge \cdots \wedge x_{2n}) = 0 \qquad i \geq 2,\ n \geq 1.$$

(voir G. Papy, Thèse ~~pas dans la lit~~. On le fait pour modules libres — sém. Cartan, puis on réécrit le module comme quotient)

M libre de rang $2n$, $u \in \Lambda^2 M$

$$Pf(u) = \text{"}\frac{u^n}{n!}\text{"} \in \Lambda^{2n} M$$

$$= \gamma_n(u)$$

<u>K-théorie de M. Milnor</u> $\quad k^M(K)$

algèbre graduée sur $\mathbb{F}_2$

générateurs (x), $x \in K^*/K^{*2} = H^1(K)$

relations $(x)(1-x) = 0$, $x \neq 0, 1$ $x \in K$.

$$\Rightarrow (x)(-x) = 0$$

comme -1 = carré, $(x)^2=0$

$$k^M(K) = \Lambda H^1(K)/J$$ J engendré par les $(x)(1-x)$.

(par certains élém. décomposables).

Lemme:

Si $J \subset \Lambda M$ est un idéal engendré par des éléments décomposables de degré 2, alors les γ_i de ΛM définissent par passage au quotient des puissances divisées sur $C = (\Lambda M/J)^{\text{pair}}$,

(définies sur élé de degré pair), $\gamma_i(x)=0$ $i\geq 2$ x décomposable.

$x \in \Lambda^{2n} M$, $y \in \Lambda^{2n} M$, $y \in J$

à vérifier : $\gamma_i(x+y) = \gamma_i(x) \bmod J$

récurrence.

Montre l'existence de puissances divisées sur $k^M(K)$ lorsque $-1 = \square$.

En particulier,

$$\begin{array}{ccc} \gamma_i : k_2^M(K) & \longrightarrow & k^M_{2i}(K) \\ \| & & \downarrow \\ H^2(K) & & H^{2i}(K) \end{array}$$

Conclusion : on a

$$\gamma_i : H^2(K) \longrightarrow H^{?i}(K)$$

$$x = \sum_{\lambda \in L} x_\lambda \qquad x_\lambda \text{ décomposables}$$

L ordonné totalement

$$\gamma_i(x) = \sum_{\lambda_1 < \cdots < \lambda_i} x_{\lambda_1} \cdots x_{\lambda_i}.$$

$i = 2$ donne $\gamma_2 = \varphi$ de tout à l'heure.

Autre façon d'obtenir φ : utiliser les puissances extérieures, λ-structure de W_K.

A algèbre centrale simple, $n = 3$

A est cyclique, $[A] = x \cdot y$ $\quad x \in H^1(K, \mu_3)$
(car $K \neq 3$). $\quad y \in H^1(K, \mathbb{Z}/3\mathbb{Z})$

Remarque : ces algèbres sont classées par $H^1(K, PGL_3)$ $\quad$ s/g naturel de type $(3,3)$
(donc Heisenberg ds GL_3)

$$\begin{pmatrix} 1 & & \\ & \rho & \\ & & \rho^2 \end{pmatrix} \quad \rho^3 = 1 \qquad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \sigma$$

$$\rho\sigma = \underset{\uparrow}{*}\, \sigma\rho$$

homothétie

On pose :
$\Phi = \mu_3 \times \mathbb{Z}/3\mathbb{Z} \hookrightarrow PGL_3$, sous-groupe d'ordre 9

$$H^1(K, \phi) \longrightarrow H^1(K, PGL_3)$$

<u>surjective</u>

$$\|$$

$$H^1(K, \mu_3) \times H^1(K, \mathbb{Z}/3\mathbb{Z}) \ni (x, y)$$

à vérifier : l'image de x, y dans

$H^1(K, PGL_3)$ est $x \cdot y$ $\quad$ (ou $-x \cdot y$??)

$\cap$

$H^2(K, \mu_3)$

(Analogue orthogonal :

$$(\pm 1) \times \cdots \times (\pm 1) \longrightarrow O_n$$

est surjectif sur H^1.)

$n = 5$: on ne sait pas si l'alg. est toujours cyclique.

<u>Formes traces des corps et des algèbres étales.</u>

car $\neq 2$

<u>Algèbres étales</u> sur K

E algèbre commutative de dim finie n sur K

(α) E isom. à un produit $\prod E_i$

E_i corps, ext. sép. de K

$\sum n_i = n$, où $n_i = [E_i : K]$.

(b) Après extension des scalaires, E devient isomorphe à $K \times \dots \times K$ (n fois).

(c) La forme trace $q_E(xy) = \mathrm{Tr}_{E/K}(xy)$ est non dégénérée.

Dictionnaire bien connu (Bourbaki)

K_s clôture séparable de K

$G_K = \mathrm{Gal}(K_s/K)$

$E \xrightarrow{\varphi} K_s$ $\quad$ K-homomorphisme

$\Phi_E = \mathrm{Hom}_{K\text{-alg}}(E, K_s)$, $|\Phi_E| = n$

action naturelle de G_K

$s \in G_K$, $\varphi \in \Phi_E$ $\quad$ $s\varphi \in \Phi_E$

action continue à gauche.

Equivalence de catégories ("th de Galois")

K-algèbres étales et ensembles finis munis d'une action continue de G_K.

(G_K-ensemble).

Comment. Math. Helv. 1984

Structure (partielle) de q_E

$n = [E:K]$, q_E : forme de rang n

On écrit $n = 2^{m_1} + \cdots + 2^{m_h}$ $\quad m_1 < m_2 < \cdots < m_h$.

1^er^ cas : $\sum m_i \equiv 0 \pmod 2$

Alors q_E contient la forme $\langle 1, \ldots, 1 \rangle$ h fois.

i.e. $q_E \cong \underbrace{\langle 1, \ldots, 1 \rangle}_{h} + g$, g de rang $n-h$.

2^ème^ cas $\quad \sum m_i \equiv 1 \pmod 2$

Alors q_E contient la forme $\langle 2, 1, \ldots, 1 \rangle$ h termes.

Démonstration est basée sur le thm de Springer

E est défini par l'action de G_K sur Φ_E, ens. à n éléments.

A isom. près, E est déterminé par

$$\varphi_E : G_K \to S_n.$$

Classes d'algèbres étales de degré n correspondent aux représentations galoisiennes

$$\varphi_E : G_K \to S_n \quad \text{à conj. près.}$$

G_E = image de G_K dans $\mathrm{Aut}(\Phi_E) \simeq S_n$

groupe de Galois associé à E

$1^{ère}$ étape

Démontrer le thm quand l'image de G_K est un 2-groupe

$2^{ème}$ étape

Ramener le cas général à celui-ci.

On choisit un 2-groupe de Sylow de G_E, et on prend son image réciproque ds G_K. C'est $G_{K'}$, avec $[K':K]$ impair.

Par le thm de Springer, il suffit de montrer la $1^{ère}$ étape.

1° Les orbites de G_K ds Φ_E sont d'ordres des puissances de 2.

Il existe une décomposition de Φ_E en sous-ensembles d'ordres $2^{m_1}, \dots, 2^{m_k}$ stables par G_K.

Décomposition de Φ_E en ss/ens. d'ordres puissances de 2, stables par G_K.

On la choisit avec nombre minimum de facteurs

$n = 2^{a_1} + \dots + 2^{a_k}$ déc. de n correspondant.

les a_i sont distincts.

Donc les $a_i = m_i$ à permutation près.

$E = E_1 \times \dots \times E_h$ $\deg E_i$ est 2^{m_i}.

$q_E = \sum q_{E_i} = \bigoplus q_{E_i}$.

$Tr_{E_i}(1^2) = 2^{m_i}$.

$q_{E_i} \cong \langle 2^{m_i} \rangle \oplus g_i$ rang $g_i = 2^{m_i} - 1$

$q_E \cong \langle 2^{m_1}, 2^{m_2}, \dots, 2^{m_h} \rangle \oplus g$

m_i pair $\Rightarrow \langle 2^{m_i} \rangle = \langle 1 \rangle$

m_i impair $\Rightarrow \langle 2^{m_i} \rangle = \langle 2 \rangle$.

De plus $\langle 2, 2 \rangle = \langle 1, 1 \rangle$. D'où le résultat.

$d(q_E) = \mathrm{disc}(E) \in K^\times / K^{\times 2} = H^1(k)$.

$n = 1, 2, 3$

$\underline{n = 2}$ $E = K(\sqrt{d})$, $q_E = \langle 2 \rangle \oplus g$

$q_E = \langle 2 \rangle \oplus \langle 2d \rangle$

$\underline{n = 3}$ $q_E \simeq \langle 1, 2, 2d \rangle$ $d = \mathrm{disc}$

Pour aller plus loin, il faut connaître l'invariant de Witt.

$w_1, w_2\ (q_E)$

$\varphi_E : G_K \longrightarrow S_n$ défini à conjugaison près.

$H^i(S_n, \mathbb{Z}/2\mathbb{Z})$ $i = 1, 2$.

$$H^1(S_n) \simeq \begin{cases} 0 & n=1 \\ \mathbb{Z}/2\mathbb{Z} & n \geq 2 \end{cases}$$

$$S_n \xrightarrow{\text{sgn}} \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$$

ε_n = élément non nul de $H^1(S_n)$

$$H^2(S_n) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & n = 2, 3 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & n \geq 4 \end{cases}$$

(Schur)

$\varepsilon_n^2 \in H^2(S_n)$
$\neq 0$

$$\begin{tikzcd} \mathbb{Z}/2\mathbb{Z} \arrow[d] & \mathbb{Z}/2\mathbb{Z} \arrow[d] \\ X \arrow[r] \arrow[d] & C_4 \arrow[d] \\ S_n \arrow[r] & \{\pm 1\} \end{tikzcd}$$

une transposition devient d'ordre 4

$\mathrm{Res}_H\, \varepsilon_n^2 \neq 0$ $\qquad H = \{(1), (12)\}$

Autre élément de $H^2(S_n)$:

$$\begin{array}{ccc} \tilde{S}_n & \longrightarrow & \tilde{O}_n(\mathbb{C}) \\ \downarrow & & \downarrow \\ S_n & \longrightarrow & O_n(\mathbb{C}) \end{array}$$

$s_n \in H^2(S_n)$

Dans l'extension $\tilde{S}_n \to S_n$ correspondante, une transposition reste d'ordre 2 mais le produit de 2 transpositions disjointes devient d'ordre 4.

$s_n = 0$ si $n \leq 3$.

s_n, ε_n^2 ind. $n \geq 4$

$$H^2(S_n) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & n = 2, 3 \quad \text{base } \varepsilon_n^2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & n \geq 4 \quad \text{base } \varepsilon_n^2, s_n \end{cases}$$

Autre définition :

$$H^i(BO_n(\mathbb{R})) \longrightarrow H^i(S_n)$$

$$H^*(BO_n(\mathbb{R})) = \mathbb{F}_2[w_1, \ldots, w_n]$$

$w_1 \mapsto \varepsilon_n \qquad w_2 \mapsto s_n$

$S_n \to O_n(\mathbb{R})$

$BS_n \to BO_n(\mathbb{R})$.

Démonstration de Schur :

S_n : présentation "à la Coxeter" de type A_{n-1} o—o—o...

$n-1$ éléments d'ordre 2, $\sigma_1, \dots, \sigma_{n-1}$

$\sigma_1 = (1\,2)$ $\quad \sigma_2 = (2\,3)$ $\quad \dots \quad \sigma_{n-1} = (n-1\ \ n)$

$\sigma_i^2 = 1$, $\quad \sigma_i \sigma_j = \sigma_j \sigma_i$ si $|i-j| \geq 2$

$(\sigma_i \sigma_j)^3 = 1$. $\quad (\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j)$

$|i-j| = 1$.

$\tilde{S}_n$ peut être présenté par des $\tilde{\sigma}_i$, $-1 \in$ centre

avec $\tilde{\sigma}_i^2 = 1$

$\tilde{\sigma}_i \tilde{\sigma}_j = -\tilde{\sigma}_j \tilde{\sigma}_i$ $\quad |i-j| \geq 2$

$(\tilde{\sigma}_i \tilde{\sigma}_j)^3 = 1$ si $|i-j| = 1$.

Pour vérifier que $\tilde{S}_n$ existe, il utilise les spineurs.

Ds $\tilde{O}_n$, on peut relever les symétries s_x où $q(x)$ est un carré.

<u>Théorème</u> (CMH, 1984).

(a) $w_1(q_E) = \varphi_E^*(\varepsilon_n)$

(b) $w_2(q_E) = \varphi_E^*(s_n) + (2)\, w_1(q_E)$

$d = \operatorname{disc} E$

$w_1(q_E) = d$

$w_2(q_E) = \varphi_E^*(s_n) + (2)(d)$.

Démonstration par torsion galoisienne

$E^{dec} = K \times \dots \times K$ n fois

$q_E^{dec} = \langle 1, \dots, 1 \rangle$ forme unité

$\varphi : G_K \to S_n = \operatorname{Aut}(E^{dec})$

φ est un 1-cocycle à valeurs ds

$\operatorname{Aut}(E^{dec})$.

E est E^{dec} tordu par φ.

$E = (E^{dec})\varphi$.

$q_E = (q_E^{dec})\varphi$

$\varphi : G_K \longrightarrow S_n \subset O_n(K)$

groupe orthogonal pour la forme unité

$$2q_E = (2q_E^{dec})\varphi$$

$$S_n \hookrightarrow O_n$$

$(ij) \longmapsto$ réflexion p.r. à $e_i - e_j$

$q(e_i - e_j) = 2$

$2q(e_i - e_j) = 4$ carré !

$$\begin{array}{ccccc} \tilde{S}_n & \hookrightarrow & \tilde{O}(2q_E^{dec}) & = & \tilde{\Sigma}(K) \\ \downarrow & & \downarrow \pi & & \downarrow \\ S_n & \subset & O(2q_E^{dec}) & = & \Sigma(K) \end{array}$$

S_n contenu dans l'image de $\tilde{\Sigma}(K)$.

<u>Lemme</u>:

<u>Soit</u> $1 \to A \to \tilde{\Sigma} \to \Sigma \to 1$

<u>une suite exacte de</u> groupes <u>algébriques</u>

$A \subset$ <u>centre</u> $\tilde{\Sigma}$, A <u>fini</u>, <u>et</u> $A(\bar{K}) = A(K)$

<u>Soit</u> $\tilde{G}$ <u>un s/g fini de</u> $\tilde{\Sigma}(K)$

<u>contenant</u> $A = A(K)$ <u>et soit</u> G

<u>son image dans</u> $\Sigma(K)$

$$\begin{array}{ccc} \tilde{G} & \subset & \tilde{\Sigma} \\ \downarrow & & \downarrow \\ G & \subset & \Sigma \end{array}$$

Alors, les 2 éléments suivants de $H^2(G_K, A)$ coïncident :

(1) φ est un 1-cocycle sur G_K, à valeurs dans Σ ; soit $[\varphi] \in H^1(K, \Sigma)$ la classe corr.

On a $\Delta : H^1(K, \Sigma) \to H^2(G_K, A)$,

d'où $\Delta[\varphi] \in H^2(G_K, A)$

(2) $\tilde{G}$ est une extension de G par A, donc définit $e \in H^2(G, A)$

$$\varphi^* e \in H^2(G_K, A)$$

On a : $\varphi^* e = \Delta[\varphi]$.

Rappelons la définition de Δ.

$\tilde{a}_s$ relève $a_s \in \Sigma(K_s)$

$$\Delta(a_s)(s,t) \longmapsto \cancel{\tilde{a}_s (\tilde{a}_{st})^{-1} \tilde{a}}$$
$$\tilde{a}_s\, {}^s\tilde{a}_t\, (\tilde{a}_{st})^{-1}.$$

ici $a_s\, \tilde{a}_s$ sont rationnels sur K.

donc

$$= \tilde{a}_s \tilde{a}_t (\tilde{a}_{st})^{-1}.$$

11 mars 1991

129

E algèbre étale de dim n sur K

carac $K \neq 2$

$q_E(x) = \mathrm{Tr}_{E/K}(x^2)$

q_E non dégénérée de rang n

$d = \mathrm{disc}(q_E) = \mathrm{disc}(E)$

$w_1(q_E) = (d) \in H^1(K)$.

$E \rightsquigarrow \varphi_E : G_K = \mathrm{Gal}(K_s/K) \to S_n$

défini à conjugaison près

$s_n \in H^2(S_n, \mathbb{Z}/2\mathbb{Z})$

$\varphi_E^*(s_n) \in H^2(G_K, \mathbb{Z}/2\mathbb{Z}) = H^2(K)$.

Théorème $\quad w_2(q_E) = \varphi_E^*(s_n) + (2)(d)$

$(q)_\alpha = q_E$, $\quad q = q^{dec}$, forme associée à $K \times \dots \times K$

$\alpha : G_K \xrightarrow[\varphi_E]{} S_n \subset O_n(K)$

$w_2(2q_E) = ?$

$O(2q_E^{dec}) = O(\langle 2, \dots, 2 \rangle) \leftarrow \tilde{O}(2q_E^{dec})$

$$\begin{tikzcd}
\Sigma \arrow[d, phantom, "\cup" description] & \tilde{\Sigma} \arrow[l] \arrow[d, phantom, "\cup" description] \\
S_n & \tilde{S}_n \arrow[l, "s_n"']
\end{tikzcd}$$

$\alpha \in H^1(K, \Sigma)$

$$1 \to C_2 \to \tilde{\Sigma} \to \Sigma \to 1$$

$$\Delta : H^1(K, \Sigma) \to H^2(K).$$

On a : $\Delta(\alpha) = \varphi_E^*(s_n)$ (lemme)

Q forme quadratique, $\alpha \in H^1(K, O(Q))$

$$w_1(Q_\alpha) = w_1(Q) + \delta^1(\alpha)$$

$$w_2(Q_\alpha) = w_2(Q) + \delta^1(\alpha) w_1(Q) + \delta^2(\alpha)$$

$$\delta^2(\alpha) = \Delta(\alpha).$$

$Q = 2q^{dec}$. $\quad w_1(Q_\alpha) = w_1(Q) + (d)$

$$w_1(2q) = w_1(\langle 2, \dots, 2\rangle) + (d)$$

d'où $w_1(q) = (d) \dots$

$$w_2(2q) = w_2(2q^{dec}) + (d) w_1(2q^{dec}) + \varphi^*(s_n)$$

Formules : $\begin{cases} w_1(\lambda q) = w_1(q) + n(\lambda) \\ w_2(\lambda q) = w_2(q) + n_1 w_1(q)(\lambda) + n_2(-1)(\lambda) \end{cases}$

où $n_1 = n-1$, $n_2 = n(n-1)/2$.

$q = \langle \alpha_1, \dots, \alpha_n \rangle$

$$w_2(\langle \lambda\alpha_1, \dots, \lambda\alpha_n\rangle) = \sum_{i<j} (\alpha_i)(\alpha_j) + (\lambda)(\alpha_i) + (\lambda)(\alpha_j) + (-1)(\lambda$$

$\lambda = 2$ donc :

$$w_2(2q) = w_2(q) + n_1(2) w_1(q)$$

$$w_2(q_E) + n_1(2)(d) = n(2)(d) + \varphi_E^*(s_n)$$

d'où la formule.

Bruno Kahn : formules pour les classes de Stiefel-Whitney supérieures, en fonction des $\varphi_E^*(w_i(s_n))$

$$S_n \to O_n(\mathbb{R})$$

$$w_i(S_n) \in H^i(S_n, \mathbb{Z}/2\mathbb{Z})$$

$w_i(q_E)$ en fonction des $\varphi_E^*(w_i(S_n))$:

$$w = \sum w_i(q_E) = \varphi_E^*(w(S_n)).(1+(2)(d))$$

Applications et cas particuliers :

Relèvement

$$\begin{array}{ccc} & & \tilde{S}_n \\ & \overset{\tilde{\varphi}}{\nearrow} & \downarrow \\ \varphi : G_K & \longrightarrow & S_n \end{array}$$

Condition de relèvement ?

Exist. de $\tilde{\varphi}$ $\iff$ $\varphi^*(s_n) = 0$

$$\overset{\shortparallel}{w_2(q_E) + (2)(d)}$$

n petit, E donné explicitement

$$E = K[X]/(f(X))$$

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n.$$

On calcule $w_2(q_E)$ en fonction des coefficients.

Méthode de Hermite - Kronecker - Klein ...

pour résoudre l'équation du $5^{\text{ème}}$ degré.

Que signifie "résoudre une équation" ?

(problème d'histoire des maths).

Supposons car$(K) \neq 2, 5$ (pas indispensable)

A_5 agit-il fidèlement sur une courbe de genre 0 ?

Vrai sur un corps algébriquement clos

$$A_5 \hookrightarrow PGL_2(K) \quad , \quad K \text{ assez gros}$$

Si un tel plongement existe, $\sqrt{5} \in K$.

Si $K \ni \sqrt{5}$, il existe une courbe de genre 0 Y sur laquelle A_5 agit.

On obtient un revêtement ramifié en 3 pts (moins en carac. 3)

$$\begin{array}{c} Y \qquad g = 0 \\ \big\downarrow \; A_5 \\ X \simeq \mathbb{P}_1 \end{array}$$

Une courbe de genre 0 a un invariant $\in H^2(K)$. Inv. de Y : $(-1)(-1)$.

($\sqrt{5} \in K$: choisissons $s \in A_5$, d'ordre 5

$$A_5 \to PGL_2(K)$$

$$Tr(s^2/\det(s)$$

$$\frac{(1+w)^2}{w} = 2 + w + w^{-1} \quad = a + b\sqrt{5}$$

K quelconque. (133)

Si $\sqrt{5} \notin K$, on obtient

Y courbe sur $K(\sqrt{5})$ munie d'une action de S_5 qui est A_5 linéaire, et semi-linéaire en dehors de A_5.

$$\begin{array}{lll} & Y & \\ & \downarrow & \\ \mathbb{P}_1/K(\sqrt{5}) & Y/A_5 & K(\sqrt{5}) \\ & \downarrow & \quad | \\ \mathbb{P}_1 & Y/S_5 & K \end{array}$$

$$\begin{array}{ccc} Y_p & \subset & Y \\ \downarrow & & \downarrow \\ p \in & Y/S_5 & = \mathbb{P}_1 \end{array}$$

$p \in Y/S_5\,(K)$

non ramifié

Y_p $\quad S_5$ - torseur sur K

$\iff G_K \to S_5$

$\iff$ algèbre étale de dim 5 sur K

$\iff$ équation de $5^{\text{ème}}$ degré (à équiv. près).

"Revêtement de Klein".

Quelles sont les équations que l'on trouve ?

Théorème :

La construction précédente donne toutes les algèbres étales de dim 5, pourvu que l'on remplace K par $K(\sqrt{\alpha}, \sqrt{\beta})$, α, β convenables.

(α, β dépendent de l'équation).

Description de Y :

1) Dans $\mathbb{P}_4$, $\sum_{i=1}^{5} x_i = 0$, $\sum_{i=1}^{5} x_i^2 = 0$

d'où une quadrique C dans $\mathbb{P}_3$ (hyperplan des $\sum x_i = 0$).

$Y =$ variété des droites de la quadrique C.

Courbe à 2 composantes connexes de genre 0

S_5 agit en permutant par la signature les 2 composantes.

C quadrique sur K. G_K agit sur l'ensemble des composantes.

(q de rg 4, corps de déf. $K(\sqrt{d(q)})$

$\langle 1, \dots, 1 \rangle = \langle 5 \rangle + \langle 5, 1, 1, 1 \rangle$

disc. 5

$G_K \longrightarrow \{\pm 1\}$ associé à $K(\sqrt{5})$.

2°) Corps des fonctions de Y (méthode modulaire).

D'abord sur $\mathbb{Q}$. Corps des fonctions modulaires de niveau 5 sur $\mathbb{Q}(\zeta_5)$

ζ_5 racine $5^{\text{ème}}$ de 1, appelé K_5.

Action de $GL(2, \mathbb{F}_5)/\{\pm 1\}$.

Invariants $\mathbb{Q}(j)$

$$\begin{array}{c} K_5 \\ | \\ \mathbb{Q}(\zeta_5, j) \\ | \\ \mathbb{Q}(j) \end{array} \qquad G_5 \text{ (tout)}, \quad \mathbb{F}_5^* \text{ (bas)}$$

$G_5 \xrightarrow{\det} \mathbb{F}_5^*$.

$\mathbb{F}_5^*/(\pm 1) \subset G_5$

2 clé

k_5 corps des invariants,

$$\begin{array}{c} k_5 \\ | \\ \mathbb{Q}j \end{array} \quad G_5/(\mathbb{F}_5^*/(\pm 1))$$

$\quad \text{''} $

$PSL(\mathbb{F}_5)$

Donc on trouve

$$
S_5 \left(\begin{array}{c} k_5 \\ | \quad A_5 \\ \mathbb{Q}(\sqrt{5})(j) \\ | \\ \mathbb{Q}(j) \end{array} \right.
$$

calcul : k_5 est de genre 0.

On a donc reconstitué la situation précédente.

Les deux constructions sont isomorphes.

(Il faudrait résoudre $\sum \theta_i = 0$, $\sum \theta_i^2 = 0$).

car $K \neq 2, 5$, $|K| \geq$ assez grand

Théorème Soit E/K une algèbre étale de dim 5, avec $(d) = (5)$.

Les propriétés suivantes sont équivalentes:

(1) E est obtenable par la construction de Klein

(2) $w_2(q_E) = (-1)(-1)$

(3) Il existe $x \in E$, $x \neq 0$, avec

$\mathrm{Tr}\, x = \mathrm{Tr}\, x^2 = 0$

(4) Il existe $f(X) = X^5 + aX^2 + bX + c$ tel que $E \simeq K[X]/(f)$.

(5) La forme $q_E \simeq \langle 5, 1, -1, 1, -1 \rangle$

$= \langle 5 \rangle + H$.

Extensions quadratiques :

- $\sqrt{5d}$ " irr. essentielle "
- Choisir ext. quadr. forçant $\mathrm{Tr}\, x = 0 = \mathrm{Tr}\, x^2$ à avoir un zéro.
  " irr. accessoire "

Brauer a vu que " irr. access. " était donné par un élé de Br_2.

$E = K.1 \oplus H$ H : éléments de Tr 0

$q_E = \langle 5 \rangle \oplus q_E'$ $q_E' = q_E / H$

$$\left[\begin{array}{l} d(q_E') = 1 \\ q_E' \text{ de rang } 4 \end{array}\right.$$

Lemme : Si Q de rang 4, $d(Q) = 1$ dans $K^\times / K^{\times 2}$.

Les 3 propriétés suivantes sont équivalentes

(a) Q repr. 0

(b) $w_2(Q) = (-1, -1)$

(c) $Q \simeq \langle 1, -1, 1, -1 \rangle$.

$q_E = q_E' + \langle 5 \rangle$

$w_2(q_E) = w_2(q_E') + (1)(5) = w_2(q_E')$.

Supposons 5. q'_E est alors hyperbolique (138)

$x \neq 0$ $\quad \mathrm{Tr}\, x = 0 = \mathrm{Tr}\, x^2 = 0$

sont les points d'une quadrique déployée/k

On veut un tel x avec $K[x] = E$ tout entier.

Sur $\overline{K}$, $E \sim \overline{K} \times \dots \times \overline{K}$.

On veut x tel que $x_1, \dots, x_5$ distinctes.

quad. dépl. $(q+1)^2$ points.

10 coniques.

Marche pour $q > 9$

Il faut vérifier $q = 3, 7, 9$

(sauf erreur, ne marche pas pour $q = 9$, marche pour $q = 3$).

1 $\Leftrightarrow$ 2 etc.

De façon générale, lorsque $\begin{matrix} Y \\ \downarrow G \\ X \end{matrix}$ est un rev. gal. fini étale,

$G_K \xrightarrow{\varphi} G$ alg. gal.

A quelle condition φ provient-il d'un point rationnel de X ?

<u>Recette</u> la variété Y_φ (tordue de Y par φ) a un point rationnel,

et l'image de ce point dans $X(K)$ convient.

On se donne $\varphi : G_K \to S_5$, on tord Y par φ. Pt rationnel ?

$Y^{déc}$ = variété des droites de la quadrique

$$\mathrm{Tr}\, x = \mathrm{Tr}\, x^2 = 0.$$

(moins points ramifiés)

Y_φ = variété des droits de la quadrique

$$\mathrm{Tr}_E\, x = \mathrm{Tr}_E\, x^2 = 0.$$

Point rationnel dessus ?

critère 3.

On peut essayer d'aller plus loin : contrôle sur invariants supérieurs.

E avec $w_1(q_E) = 0$ d carré $\varphi_E : G_K \to A_n$

$w_2(q_E) = 0$ φ_E relevable dans $\tilde{A}_n$

On a une forme quadratique q_E avec

q_E et $q_E^{dec} = \langle 1, \dots, 1 \rangle$ mêmes w_1, w_2

$$q_E - q_E^{dec} \in I_K^3 \longrightarrow H^3(K)$$

$i_3(E)$ = image de $q_E - \langle 1, \ldots, 1\rangle$

dans $H^3(K)$.

calculer $i_3(E)$?

Premier cas intéressant : $n = 6$.

$\varphi_E : G_K \to \tilde{A}_6$

$H^i(\tilde{A}_6, \mathbb{Z}/2\mathbb{Z})$: cohomology stable du 2-groupe de Sylow.

$S_2(A_6) = D_4$

On trouve : $H^1 = H^2 = 0$ pour $\tilde{A}_6$

$H^3(\tilde{A}_6, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$

(vrai pour $\tilde{A}_n$?)

(Nakaoka ~1950)

Soit u la classe non triviale de $H^3(\tilde{A}_6)$

$\varphi : G_K \to \tilde{A}_6$

$\varphi^* u \in H^3(K)$.

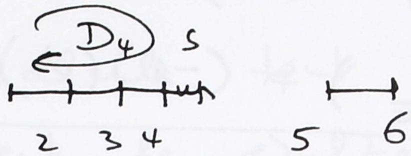
Est-ce que $i_3(E) = \varphi^*(u)$?

Vrai si $\sqrt{2} \in K$ (mais en fait cet invariant est toujours 0 !).

Principe basé sur le théorème de Springer.

On peut supposer que $\varphi(G_k) \subset S_2(\tilde{A}_6)$

$\varphi_E(G_k) \subset S_2(A_6) = D_4$



$\leftarrow$ sign. 1

$D_4 \hookrightarrow S_4$, $D_4 \hookrightarrow S_2$, combinés pour sign. 1.

On peut calculer la forme quadratique grâce à ça.

Question liée : $\underline{n = 6}$

S_6 a un automorphisme externe

$$\mathrm{Out}(S_6) = \mathbb{Z}/2\mathbb{Z}$$

(alors que $\mathrm{Out}(S_n) = \{1\}$ pour $n \neq 6$).

$\sigma \in \mathrm{Out}(S_6)$, non dans S_6

E algèbre étale, $\varphi : G_k \to S_6$

$$\downarrow \sigma$$

$\sigma \varphi_E = \varphi_{E'}$ $\qquad S_6$

algèbre étale

"Résolvante sextique" d'un polynôme de degré 6

$f_6 \mapsto f_6'$ tel que, génériquement, si

Comment comparer q_E et $q_{E'}$?

$$\boxed{\begin{aligned} w_1(q_{E'}) &= w_1(q_E) = (d) \\ w_2(q_{E'}) &= w_2(q_E) + (-1)(d) \end{aligned}}$$

$H^i(S_6)$, $i = 1, 2$ action de l'automorphisme externe

sur $H^1(S_6) = \mathbb{Z}/2$ action est triviale

sur $H^2(S_6)$ action non triviale

base ε_6^2, s_6

action de l'élément non trivial de $\mathrm{Out}(S_6)$

est
$$\varepsilon_6^2 \longmapsto \varepsilon_6^2$$
$$s_6 \longmapsto s_6 + \varepsilon_6^2.$$

$$(12) \mapsto (12)(34)(56).$$

Supposons $(d) = (1)$, $\varphi_E(G_k) \subset A_6$.

Théorème : $\boxed{q_{E'} \cong 2q_E}$.

On peut donner des exemples où $q_{E'} \not\cong q_E$, bien que ces formes aient les mêmes w_1, w_2.

Sur un corps de nombres, $q_E \cong q_{E'}$.

Principe de la démonstration :

On peut supposer, par le théorème de Springer, que $\varphi_E(G_k) \subset S_2(A_6) = D_4$.

$$E = K_4 \times K_2$$
$$\quad D_4 \quad D_2$$

On calcule tout explicitement, et on obtient le résultat.

(Il y a aussi une autre démonstration)

Autre cas analogue :

Groupe d'ordre 168, $G = SL_3(\mathbb{F}_2) = PSL_2(\mathbb{F}_7)$

Représentation naturelle $G \xrightarrow{\rho} A_7$
$\qquad\qquad\qquad\qquad\qquad\quad \xrightarrow{\rho'} A_7$

$\mathrm{Aut}((2,2,2))$

action sur 7 points $\rightarrow \rho$ et ρ'.
$\qquad\quad$ 7 droites

D'où $\varphi : G_K \longrightarrow G$ $\begin{matrix} \nearrow A_7 \\ \searrow A_7 \end{matrix}$

d'où 2 algèbres ~~[illegible]~~ étales de rang 7, E et $\widehat{E}$.

Facile à voir que q_E et $q_{\widehat{E}}$ ont le même w_1 $(=0)$

— " — $\qquad w_2$

Théorème :

On a $q_E \cong \langle 1 \rangle \oplus \varphi_6$

$$q_{\hat{E}} \cong \langle 1 \rangle \oplus 2\varphi_6$$

où φ_6 est de rang 6.

On a : $q_E \cong \langle 1 \rangle \oplus \underbrace{\langle 1 \rangle \oplus \langle 2 \rangle \oplus \psi_4}_{\varphi_6}$

Ceci découle du thm sur A_6.

Par Springer, on peut supposer que

$\varphi(G_K) \subset S_2(G) = D_4$

$$\begin{tikzcd} D_4 \arrow[r, hook] & A_6 \arrow[r, hook] \arrow[d, "\text{aut. ext}"] & A_7 \\ & A_6 \arrow[ur] & \end{tikzcd}$$

fixant 1 pt

$$D_4 \to A_6 \xrightarrow[\text{ext}]{} A_6 \to A_7$$

$E = K \times E_6$, $E' = K \times E'_6$

$q_E = \langle 1 \rangle \oplus q_{E_6}$ $\qquad$ $q_{E'} = \langle 1 \rangle \oplus q_{E'_6}$

$$\Rightarrow q_{E'_6} \cong 2\, q_{E_6}.$$

Retour sur l'exemple quintique :

$|K| = 9$ les coniques sont en fait non disjointes

corps $\mathbb{F}_3, \mathbb{F}_7, \mathbb{F}_9$ E algèbre étale de rg 5 sur K

disc 5 (mod □) est de la forme

$K[X] / X^5 + a_1 X^4 + \dots + a_5$

avec $a_1 = a_2 = 0$.

classe de conjugaison $c \in S_5$

Quand 5 est un carré ($q = 9$), c doit être ds A_5

~~n' pas~~ ($q = 3$ ou 7), c —— ds $S_5 - A$

ds A_5 $c = (1), (12)(34), (123), (12345)$

ds $S_5 - A_5$ $c = (12), (123)(45), (1234)$.

i.e.

$E = \underbrace{\mathbb{F}_9 \times \dots \times \mathbb{F}_9}_{5 \text{ fois}}, \mathbb{F}_{9^2} \times \mathbb{F}_{9^2} \times \mathbb{F}_9, \mathbb{F}_{9^3} \times \mathbb{F}_9 \times \mathbb{F}_9, \mathbb{F}_9$

et resp $E = \mathbb{F}_{q^2} \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_{q^3} \times \mathbb{F}_{q^2}, \mathbb{F}_{q^4} \times \mathbb{F}_q$.

On est amené à trouver les polynômes correspdts

Exemple $q = 3$

$$F = \underbrace{(X^3 - X)}_{\substack{\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \\ (3 \text{ racines})}} \underbrace{(X^2 + 1)}_{\mathbb{F}_{q^2}} = X^5 - X$$

$$f = \underbrace{(X^3 - X + 1)}_{\substack{\text{irred de} \\ d^o 3}} \underbrace{(X^2 + 1)}_{\mathbb{F}_{q^2}} = X^5 + X^2 - X + 1$$

$$f = \underbrace{(X^4 + X - 1)}_{\text{irred de } d^o 4} X$$

Algèbres à involution

K car K ≠ 2

A K-algèbre associative, élt unité, de dimension finie ≥ 1 munie d'un anti-automorphisme involutif $x \mapsto x^*$ (ou x^J, x^I, ...)

$$\begin{cases} x \mapsto x^* \text{ est } K\text{-linéaire} \\ (xy)^* = y^* x^* \\ (x^*)^* = x \end{cases}$$

Structure r = radical de A

il est stable par $x \mapsto x^*$

$0 \to r \to A \to B \to 0$

$B = A/r$ s. simple

C = centre de B (stable par l'involution)

$C = \prod_{\alpha \in \Sigma} K_\alpha$ K_α ext. finies de K.

Cette décomposition est "stable par l'involution"

l'involution opère sur Σ.

d'où une déc. $C = \prod_{\beta \text{ fixe}} K_\beta \times \prod_{\substack{\gamma \text{ et } \gamma' \neq \\ \text{échgés}}} (K_\gamma \times K_{\gamma'})$

L'algèbre B est aussi découpée en

$$B = \prod B_\beta \times \prod_{\substack{\gamma \text{ ens} \\ \text{de représ.} \\ \text{"}\gamma^* \neq \gamma\text{"}}} B_\gamma$$

centre de B_β est K_β un corps, B_β simple

centre de B_γ est $K_\gamma \times K_{\gamma'}$ (échgés par involution)

B_γ simple.

L'involution dans le 1^e cas (B_β) opère sur K_β.
Dans le second cas, elle échange K_γ et $K_{\gamma'}$.
sur K_β :
action triviale ou par K_β / K^0_β quadratique.

Hypothèse provisoire K algt clos
A semi-simple, indécomposable comme alg à involution

2 cas : ① centre de A est un corps K
$A \simeq M_n(K)$
② centre de A est $K \times K$
$A \simeq M_n(K) \times M_n(K)$
les 2 copies st échangées par l'involution

① :
$x \longmapsto x^*$ anti-automorphisme
Or $x \longmapsto {}^t x$ est involution
On sait que les automorphismes st intérieurs $x \mapsto yxy^{-1}$
Donc il existe $y \in A^{*\times}$, tq
$$x^* = y\,{}^t x\, y^{-1}$$
$$x^{**} = y(y\,{}^t x\, y^{-1})^t y^{-1} = y\,{}^t y^{-1}\, x\, {}^t y\, y^{-1}$$
donc ${}^t y\, y^{-1} = \lambda \in K^\times$ $\quad {}^t y = \lambda y$ donc $\lambda = \pm 1$

d'où 2 possibilités $\lambda = 1$, $y = {}^t y$ cas orthogonal
$\lambda = -1$, $y = -{}^t y$ cas symplect.
ceci n'est possible que si n pair

② Si on identifie le 1^{er} morceau, ops le second tel que $(x, y) \mapsto ({}^t y, {}^t x)$.

K non algr clos

A simple (comme alg. à involution)

Le centre de A est L ou $L \times L$.

① L fixé par involution

L comme corps de base

$A \otimes_L L_s \simeq M_n(L_s)$ avec invol^t. orthog ou symp.

② L non fixé

L_0 sous corps fixé

$A \otimes_{L_0} L_s$ est du 2^e type

③ $L \times L$

$A \simeq B \times B^0$ B alg. simple centrale

les deux facteurs étant échangés par l'involution

Cas séparabt clos

Automorphismes d'une telle algèbre

$M_n(K)$ type orthogonal ; similitudes / homoth

symplectique "

$M_n(K) \times M_n(K)$ composante neutre d'indice 2 qui est PGl_n

n impair Toute similitude est produit d'un scalaire et d'une tr orth.

n pair 2 types $\langle sx, sy \rangle = \lambda \langle x, y \rangle$

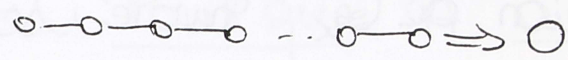
$n = 2m$ dét $(s) = \pm \lambda^m$

type 1 simil / homoth → $\begin{cases} n \text{ impair} & \mathrm{Aut} = O_n/\pm 1 = SO_n \\ n \text{ pair} & \mathrm{Aut}^0 \text{ indice } 2 \text{ ds } \mathrm{Aut} \\ & \mathrm{Aut}^0 = O_n/(\pm 1) \end{cases}$

type symplect. → $\begin{cases} \mathrm{Aut}^0 = O_n/\pm 1 \\ \mathrm{Aut} = Sp_n/\pm 1 \end{cases}$

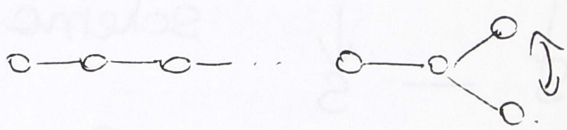
2 comp → $\begin{cases} \mathrm{Aut}^0 \text{ indice } 2 \\ \mathrm{Aut}^0 = PGl_n \end{cases}$

<u>Comparaison</u> <u>aux</u> <u>diagrammes</u> <u>de Dynkin</u> (des groupes classiques)

type 1 n impair $B_{\frac{n-1}{2}}$ 

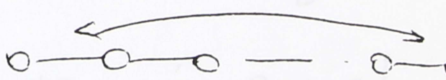
$n \neq 1$

pas d'autom. externes.
c'est connexe.

n pair $D_{\frac{n}{2}}$ 

$n \neq 4, 2, 8$

type sympl. $C_{n/2}$ 

type 2 compos. A_{n-1} 

$n \neq 1, 2$

K A algèbre déployée simple.
(comme algèbre associative).
cas orthogonal : forme standard = $\left|\begin{array}{l}\text{hyperbol. si } n \text{ pair} \\ \langle 1\rangle + \text{hyperb si non}\end{array}\right.$

A → gpe simple (adj^t) = comp neutre
/ de Aut A
déployé.
G de l'un des types
classiques.

On a ainsi un isomorphisme de Aut A $\to$ Aut G.
[Weil, OC, II] Les K-formes de A correspondent aux K-formes de G.

<u>A l'exception des formes de D_4</u> "trialitaires" <u>toute</u> K- <u>forme d'un groupe classique</u> (simple abs^t) <u>s'obtient à partir d'une alg. à involution</u> ("simple de centre K").

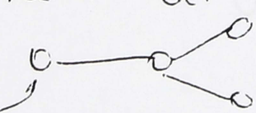
Action de G_K sur le schéma :

K

diag de D_4

$$\begin{array}{ccc} G & & S' \\ \big| & & \downarrow \\ S & - & S \end{array}$$

schéma des schémas de Dynkin

trialitaire : les 3 sommets ext. st permutés.
sinon 1 sommet fixé  et on a alg. à involution.

Voilà pourquoi on s'intéresse aux algèbres à involution - elles fournissent toutes les formes des groupes classiques !

Théorème (Albert)

Soit A une algèbre centrale simple sur K. Pour que A possède une involution (fixant K), il faut et il suffit que $2[A]=0$ ds $Br(K)$.

Théorème (Albert)

Soit L/K une ext. quadratique et soit A une L-algèbre simple centrale. Pour que A ait une K-involution non triviale sur L, il faut et il suffit que $Cor_{L/K}[A]_L = 0$ ds $Br(K)$.

Démonstration du 1er théorème

$*$ définit un isomorphisme $A \to A^{\circ}$ alg opposée

donc $[A] = [A^{\circ}]$ ds $Br(K)$
$= -[A]$

Réciproquement, (supposons que) $[A] = [A^{\circ}]$.

On peut supposer que A est un corps gauche car $A = M_n(D)$ D alg à division et une involution sur D se prolonge à A à savoir $(d_{ij}) \to (d_{ji}^*)$

Soit L un ss corps séparable commutatif maximal de A

$[A:K] = n^2 \Rightarrow [L:K] = n$

Lemme (a) Il existe un anti-isomorphisme $A \to A$ qui est l'identité sur L.

(b) Un tel anti-isomorphisme est une involution.

(a) Choisissons un anti-isomorphisme $x \mapsto i(x)$ de A

i_L = rest. de i à L est un isomorphisme de L sur $i(L)$.

Donc il existe (Skolem-Noether) $a \in A^\times$ tel que $i(x) = a x a^{-1}$ pour tout x de L.

L'antiisomorphisme $x \mapsto a^{-1} i(x) a$ possède la propriété voulue en a)

(b) est un énoncé géométrique. il se vérifie après ext. des scalaires, Alors A devient $M_n(K)$ et L devient l'algèbre diagonale $K \times \_ \times K \hookrightarrow M_n$

Soit i un anti-isomorphisme $A \to A$.

Il existe $a \in A^\times$ tq $i(x) = a^t x a^{-1}$.

$a^t x a^{-1} = x \quad x \in L$

$\Longrightarrow$ a commute à L

$\Longrightarrow$ $a \in L^\times \qquad a = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$

d'où $i^2(x) = a({}^t a^{-1}\, x\, {}^t a) a^{-1} = x$.

Si $[A] = [A^\circ] \Rightarrow$ involution existe | de type $\perp$ (n quelconque) / de type alterné (n pair)

La méthode donne $\perp$ par construction.

Pour le type alterné, il s'en déduit :

on choisit $a \in A^\times$ avec $a^* = -a$ (existe si n pair) (si $*$ type $\perp$,)

$x^I = a x^* a^{-1}$ définit une involution de type symplectique.

Reste à choisir $a \in A^\times$ $a^* = -a$

$a \in A^\times$: donne un ouvert de Zariski de A.

Supposons K infini

Soit A_- l'ensemble des éléments anti-invariants par $*$. On doit voir que A_- rencontre cet ouvert
Il suffit de le voir après extension des scalaires
OK si n pair.

Si K fini A est une alg. de matrices
d'où existe de formes alt non dégénérées
si n pair.

<u>Remarque</u>: A invol. simple de centre K $rg = n^2$

$A_+ = \{a, a^* = a\}$ $\dim A_+ = \dfrac{n(n+1)}{2}$
dans le cas orthogonal

$= \dfrac{n(n-1)}{2}$

dans le cas symplectique

<u>2e thme : preuve</u>

A centrale simple sur L, L/K quadratique
K- involutions de 2e espèce, non triviales sur L

A sur L

$\lambda \mapsto \bar\lambda$ invol de L

① $\bar A$ algèbre réduite de A par changement de base $L \xrightarrow[\lambda \mapsto \bar\lambda]{} L$.

② A vue comme L-algèbre par $L \xrightarrow{-} L \to A$.

③ $\bar{a} \in \bar{A}$

$\overline{(ab)} = \bar{a}\,\bar{b}$

$\overline{\lambda a} = \bar{\lambda}\,\bar{a} \quad \lambda \in L$

Une involution de 2^e espèce définit un anti-isomorphisme $A \longrightarrow \bar{A}$, ie $A^o \simeq \bar{A}$.

d'où condition nécessaire ds Br

$$[A^o] = [\bar{A}] \text{ ds } Br(L)$$

ie $\quad [A] + [\bar{A}] = 0 \qquad (+)$

Soit A satisfaisant à $[A] + [\bar{A}] = 0$.

Il existe $\quad i : A \longrightarrow A$ tq $\quad i(x.y) = i(y)\,i(x)$

$\qquad i(\lambda) = \bar{\lambda} \quad \lambda \in L$

i : anti-linéaire
anti-isomorphisme.

Si i est comme ci-dessus,

$x \longmapsto i^2(x)$ L-automorphisme de A

Il existe $a \in A^\times$ tq $i^2(x) = a x a^{-1}$. $\forall x \in A$

$$i^3(x) = i\,(i^2(x)) = i(a^{-1})\,i(x)\,i(a)$$

$$= i^2\,(i(x)) = a\,i(x)\,a^{-1}.$$

$\Rightarrow$ Il existe $\lambda \in L^\times \quad \lambda = a\,i(a)$

$\qquad = i(a)\,a$

$$i(\lambda) = i^2(a)\,i(a) = a\,i(a) = \lambda$$

donc $\lambda \in K^\times$.

Que donnent d'autres choix?

$a \mapsto \mu a \quad \mu \in L^\times \quad \lambda$ défini à $NL^\times$ près.

On peut aussi changer de i, mais en fait :

λ vu comme élt de $K^\times / NL^\times$ ne dépend ni du chx de a, ni de celui de i.

$i'(x) = b i(x) b^{-1}$ et calcul. (cf Scharlau)

$K^\times / NL^\times = Br(L|K) = \mathrm{Ker} : Br\, K \to Br\, L$.

<u>Lemme</u>. <u>L'élément</u> $\underset{(L/K,\lambda)}{\underset{\uparrow}{(\lambda)}} \in Br(L|K)$ <u>est la</u> $\mathrm{Cor}_{L|K}[A]$

Si une invol existe, $a = 1 \quad \lambda = 1 \Rightarrow \mathrm{Cor} = 0$

Invers^t si $\mathrm{Cor} = 0$, $\lambda = \mu \bar{\mu}$

on chge pr que $\lambda = 1$, $a i(a) = 1$.

on chge de i ! :

$i \mapsto b i b^{-1} \quad J(x) = b i(x) b^{-1}$

$J^2(x) =$

(voir p. 158, Correction) $= b\, i(b^{-1})\, a x a^{-1} i(b) b^{-1}$

d'où $b\, i(b^{-1}) = a^{-1}$ ie $a \in \mathrm{Im}(i-1)$. OK

<u>Preuve du lemme</u> B alg sur L (quad $/K$)

$\mathrm{Vect}_L \longrightarrow \mathrm{Vect}_{|K}$

$V \otimes_L \bar{V}$ $\quad \mathrm{Gal}(L|K)$ opère semi-linéairement par $x \otimes \bar{y} \mapsto y \otimes \bar{x}$

d'où "K-structure"

On appelle W les éléments invariants

K-esp. vectoriel

$W = \mathrm{Cor}_{L|K} V$

Se définit plus généralement dès que $L|K$ séparable et descente à Weil.

On devrait appeler ceci $N_{L|K} V$ "norme" de V.

[Par contre $\mathrm{Tr}_{L|K} V = V$ vu comme K-esp vectoriel obtenu par descente à partir de la somme directe des conjugués.]

On a $N(V \otimes V') = N(V) \otimes N(V')$.

B alg sur L $\longrightarrow$ $\mathrm{Cor}\, B$ = s K-algèb de $B \otimes_L \overline{B}$ formée des invariants de $\sum b_i \otimes \overline{c_j} \mapsto \sum c_j \otimes \overline{b_i}$

(cf Riehm, Inv.).

$A \otimes_L \overline{A} = \Delta \otimes_K L$ $\qquad$ $\Delta = \mathrm{Cores}\, A$

algèbre centrale simple sur K

H alg de quaternions définie par $(L|K, \lambda)$

$H = L \oplus L.\varphi$ $\qquad$ $\varphi^2 = \lambda$

$\varphi l \varphi^{-1} = \overline{l}$ pour tout $l \in L$

On va voir que $\Delta \otimes_K H$ est isomorphe à une alg. de matrices, d'où $[\Delta] + [H] = 0 \Rightarrow [\Delta] = [H]$

On a: $\dim_K \Delta = n^2$ $\qquad$ $\dim_K H = 4$

$\dim_K A = 2n$

On définit deux plongements

$$\Delta \longrightarrow \mathrm{End}_K A \,(\simeq M_{2n}(K))$$

$$H \longrightarrow \mathrm{End}_K A$$

de sorte que les images soient le commutant l'une de l'autre d'où isomorphisme voulu

$$\Delta \otimes_K H \simeq \mathrm{End}_K A.$$

(car les dimensions sont bonnes).

$$\Delta \subset A \otimes \overline{A}$$

$$A \otimes_L \overline{A} \longrightarrow \mathrm{End}_K A$$

$$x \otimes \overline{y} \longmapsto u_{x,\overline{y}}(z) = x\, z\, i^{-1}(y) \qquad z \in A$$

$$H = L \oplus L\varphi \qquad \varphi^2 = \lambda$$

$$L \longrightarrow \mathrm{End}\ A$$

$$\varphi \longmapsto \underline{\varphi} \in \mathrm{End}\ A \qquad \underline{\varphi}(z) = i(z)\, a \quad z \in A$$

Vérifions. $\underline{\varphi}^2(z) = i(\,i(z)\,a)\,a = i(a)\,i^2(z)\,a = \quad i(a)\,a\,z\,a^{-1}a = \lambda z.$

On a de plus $u_{x,\overline{y}} \circ \varphi = \varphi \circ u_{y,\overline{x}}$, d'où le fait que les images de Δ et de H dans $\mathrm{End}_K(A)$ commutent. D'où le résultat cherché.

1) <u>Corrections</u>: corps fini, il est préférable de supposer $q>6$, car $E \simeq k[X]/(f)$.

"type de Klein"

on ne peut pas prendre un pt de ramification pour relever (ce qui ~~impose~~ $q \geq 62$) $\downarrow^{A_5}$ $\mathbb{P}_1$

et peut-être mieux. marche dès que

2) A <u>de</u> 2e <u>espèce</u> $aa^* = 1 \Rightarrow a \overset{?}{=} b^{-1}b^*$

① On pourrait supposer que A est un corps (gauche) Car = 0.

② Si $a = -1 \Rightarrow i^2(x) = axa^{-1} = x$, i involution

③ Si $1+a$ est inversible et $b = \frac{1}{1+a}$ convient

$$b^* = \frac{1}{1+a^{-1}} = \frac{a}{1+a} \qquad b^{-1}b^* = a$$

A est une k-algèbre à involution $*$, car $k \neq 2$

éléments <u>hermitiens</u> (ou symétriques) $a^* = a$: H_A

<u>antihermitiens</u> A_- $\quad A = A_- \oplus H_A$

<u>unitaires</u> U_A : $a^*a = 1$.

On souligne les lettres pour indiquer les variétés algébriques correspondantes

$\underline{H}_A(k) = H_A$

$\underline{H}_A(k') = H_{A \otimes_k k'}$

$\underline{U}_A \subset Gl_A$ (groupe multiplicatif de A)

$Gl_A(K') = (A \otimes_K K')^\times$

hermitiens inversibles $\underline{H}_A^\times$.

Th: $\boxed{Gl_A / \underline{U}_A \simeq \underline{H}_A^\times}$ (comme variétés algébriques)

$x \in Gl_A$ $h \in \underline{H}_A$ $x h x^* \in H_A$ d'où une action de Gl_A sur $\underline{H}_A$ (en particulier $\underline{H}_A^\times$).

L'action sur $\underline{H}_A^\times$ est transitive et le stabilisateur de $h = 1$ est $\underline{U}_A$.

montrer:

$$Gl_A \longrightarrow \underline{H}_A^\times \quad \text{lisse}$$

$$x \longmapsto x \cdot 1 \cdot x^* = x x^*$$

L'application tangente à l'origine:

$x = 1 + \varepsilon$ $\qquad$ $A \longrightarrow \underline{H}_A$

$\begin{cases} \varepsilon^2 = 0 \\ \varepsilon\varepsilon^* = 0 \end{cases}$ $\qquad$ $\varepsilon \longmapsto \varepsilon + \varepsilon^*$

$(1+\varepsilon)(1+\varepsilon^*) = \ldots$ $\qquad$ surjective

car: $\varepsilon + \varepsilon^* = \eta$ $\quad \varepsilon = \frac{\eta}{2}$ marche

Plus généralement:

$$Gl_A \longrightarrow \underline{H}_A^*$$

$$x \longmapsto x h x^* \qquad h \in H_A^\times$$

L'appl. tgle est $\varepsilon \longmapsto \varepsilon h + h\varepsilon^*$, est aussi surjective

[Si $\eta \in H_A$ on pose $\varepsilon = \frac{1}{2}\eta h^{-1}$, et l'on a:

$$\varepsilon h + h\varepsilon^* = \frac{1}{2}\eta + \frac{1}{2} h(h^{*-1}\eta^*)$$

$$= \frac{1}{2}\eta + \frac{1}{2}\eta = \eta.]$$

l'appl. tgte est surjective, les orbites sont ouvertes

$H_A^\times$ ouvert d'un ev., irréductible, connexe donc il y a une seule orbite. D'où le résultat

Tout élt hermitien inversible est donc du type $x x^*$ après extension des scalaires.

Ce point se démontre en fait directement: si K algt clos, tout hermitien inv. est le carré d'un hermitien. En effet

<u>Lemme</u> <u>Si</u> K algt <u>clos</u> de car $\neq 2$ et si E est <u>une alg. de dim finie</u> sur K, <u>H élt inversible</u> <u>de</u> E <u>est un carré</u>.

(On applique à E = alg eng. par un élt hermitien

$$1 \longrightarrow \underline{U}_A \longrightarrow Gl_A \longrightarrow \underline{H}_A^\times \longrightarrow 1$$

espace homogène

$$A^\times \to H^0(K, \underline{H}_A^\times) \to H^1(K, \underline{U}_A) \longrightarrow H^1(K, Gl_A)$$

$$\underset{H_A^\times}{\parallel} \qquad\qquad \underset{0}{\parallel} \text{ "thme 90"}$$

cf LN 5 Interprétation de la suite exacte:

$$\boxed{H^1(K, \underline{U}_A) \simeq H_A^\times / \text{action de } A^\times}$$

action de $A^\times$: $a \in A^\times$ $h \mapsto a h a^*$

classes de modules hermitiens de rang 1 non dégénérés $\simeq H^1(K, \underline{U}_A)$

M A-module à gauche (de type fini)

A forme hermitienne sur M

$h : M \times M \to A$

$h(am_1, m_2) = a\,h(m_1, m_2)$

$h(m_1, am_2) = h(m_1, m_2)\,a^*$

$h(m_1, m_2) = h(m_2, m_1)^*$

$a \in A \quad m_i \in M$

A non dégénérée : si $m_1 \in M$ est orthogonal à tout m $(h(m_1, M) = 0)$, alors $m_1 = 0$.

(Rappel : on est ds le cas de dim finie !).

Cas particulier M libre de rang 1. $M = Ae$

$h(e,e)$ suffit pour tout connaître

$h = h(e,e) \in H_A^\times$

Chgt de base le transforme en $a h a^*$

Aut A "voisin" du groupe des automorphismes des groupes simples classiques.

$$U_A \longrightarrow \mathrm{Aut}\, A$$

$x \in U_A \quad x \mapsto u x u^*$ est un automorphisme de $(A, *)$.

Si A est semi-simple de centre étale (un produit d'extensions séparables de K), l'image de U_A dans Aut A est ouverte.

Noyau = centre de U_A.

① { Le "Principe de Hasse" pour les corps de nombres n'est pas toujours vrai pour U_A.

K corps de nombres

$$H^1(K, \underline{U}_A) \longrightarrow \prod_v H^1(K_v, U_A)$$

n'est pas toujours injective

Exercice : A algèbre de quaternions sur K

$*$ = involution de A différente de l'involution standard.

$\dim \underline{U}_A = 1$ 2 comp. connexes

celle de l'élt neutre est un tore

[Soit $a \in A^\times$ avec $\bar{a} = -a$ ("$-$" = invol. stand)

On pose : $x^* = a \bar{x} a^{-1}$.]

Par un choix convenable de l'involution (bcp de places ramifiées, au - 4 marche).

principe de Hasse faux ("c'est le seul cas").

② <u>Invariants de tenseurs quadratiques</u>

V esp. vect. de dim finie sur K

Soient v_λ des "tenseurs quadratiques" ie des éléments de $\otimes^2 V$, $V \otimes V'$, $\otimes^2 V'$.

Soit G_v le fixateur de ces éléments $\subset GL_V$

Alors G_v est isomorphe au groupe unitaire $\underline{U}_A$ d'une algèbre à invol. convenable

Cor intersection de gpes orthog (et symplectiques) est un gpe unitaire.

<u>Rque</u>: <u>cubique ne marche pas</u>

- G_2 rep. irréd d° 7 forme trilinéaire alternée $\longrightarrow G_2 \times \mu_3$
- E_6 est aussi possible (rep. de d° 27).

Application par Eva à ex de pcpe Hasse faux.

<u>Preuve de ②</u>:

On va construire une alg. à involut A

$A \subset End(V) \times End(V') = R$ $\quad V' =$ dual

$$(f, g) \longmapsto ({}^t g, {}^t f)$$

Pour tout tenseur v quadratique, on va définir $A_v \subset R$

ⓐ $v \in V \otimes V' = End(V)$

$$V \xrightarrow{v} V$$

$A_v = \{ (f,g),$ avec $fv = vf$, et ${}^t g v = v\, {}^t g \}$.

(f,g)

fixateur de v est égal à U_{A_v}

ici $f v f^{-1} = v$

$fv = vf$

$U_R = \{ (f, {}^t f^{-1}) \} \quad f \in Gl(V)$

(b) $v \in V \otimes V = \mathrm{Hom}(V, V')$

$$\begin{array}{ccc} V & \xrightarrow{v} & V' \\ f \downarrow & & \downarrow g \\ V & \xrightarrow[v]{} & V' \end{array} \qquad A_v = \left\{ (f,g) \mid \begin{array}{l} gv = vf \\ {}^t f v = v\, {}^t g \end{array} \right\}$$

On vérifie que ceci définit alg à invol et que le fixateur est le gpe unitaire

grâce aux "2 cond" ne dépend pas de la manière de voir v comme hom.

(c) $v \in V' \otimes V'$ m chose

ou encore v interprété comme forme bilinéaire

$B_v : V \times V \to K$

$$(f,g) \in R_v \iff \left\{ \begin{array}{l} B_v(fx, y) = B_v(x, {}^t g y) \\ B_v(gx, y) = B_v(x, {}^t f y) \end{array} \right. \quad \forall x, y.$$

Problème

Existe-t-il un plongement de G_2 dans un groupe semi-simple G et des ss gpes H_λ de G isom à ss gpe orth (ou sympl.) tels que $G_2 = \cap H_\lambda$?

(En particul. on ne demande plus Algt général ds un Gl avec l'ident usuelle).
en g.al : on plonge ds $\cap$ quadriques.

Théorème (Bayer-Lenstra) Soit A une K algèbre à invol. Soit $K'|K$ une ext de d^o impair
Alors $H^1(K, \underline{U}_A) \longrightarrow H^1(K', \underline{U}_A)$ est injective.

Plusieurs réductions

→ radical
$r_A \subset A$ $\begin{cases} A/r_A & \text{semi-simple} \\ r_A & \text{idéal nilpotent} \end{cases}$

Th : $H^1(K, \underline{U}_A) \longrightarrow H^1(K, \underline{U}_{A/r})$ est bijective

Par ex : en interprétant avec les hermitiens (inversible $\Leftrightarrow$ image mod rad inv.).
Ou encore
$$1 \to N \to \underline{U}_A \to \underline{U}_{A/r} \to 1,$$
N = unipotent déployé = ext. succ. de $\mathbb{G}_a$ donc à cohom. triviale.

On peut supposer $K' = K(x)$ monogène

On choisit un tel x, d'où une forme linéaire $\lambda : K' \to K$, $\lambda(1) = 1$ et $\lambda(x^i) = 0$, $1 \leq i \leq n-1$

M_1 et M_2 modules hermitiens sur A non dégénérée libre de rang 1.

$K' \otimes M_1 \simeq K' \otimes M_2 \Longrightarrow M_1 \simeq M_2$

Si M' est un A'-module hermitien de rang 1, on définit $\lambda(M')$, A-module hermitien de rang $n = [K' : K]$ par :

($A' = K' \otimes_K A$)

$\lambda(M') = M'$ comme A-module

$$\begin{tikzcd} M' \times M' \arrow[rr] \arrow[dr] & & A \\ & A' \arrow[ur, "\lambda \otimes 1"'] & \end{tikzcd}$$

($A' = K' \otimes A$)

$M'_1 = K' \otimes M_1$

$\downarrow$

$N_1 = \lambda(M'_1)$ de rang n sur A.

On peut donner la structure de ce module

K' esp. quad. sur K

$(x, y) \longmapsto \lambda(xy)$

$$K' \simeq \langle 1,1,-1,1,-1,-,1,-1\rangle$$

$$\simeq \langle 1\rangle + \underset{\text{hyperbolique}}{h}$$

$$K' = K1 \oplus H' \oplus H''$$

totalt isot

$$N_1 \simeq M_1 \oplus \underbrace{\underbrace{H'_1}\oplus\underbrace{H''_1}}_{\substack{\text{totalt isotropes}\\ \text{libres de rg } \frac{m-1}{2}}}$$

idem pour N_2

$$H'_1 \oplus H''_1 \simeq H'_2 \oplus H''_2$$

Thme de simplification de Witt est vrai ds le cas hermitien (cf exposé d'Eva ci-après).

d'où $M_1 \simeq M_2$

" Eva Bayer.
Thme de Witt hermitien"

Fin de la réduction

$$H^1(K, U_A) \to H^1(K', U_A) \quad \text{injective}$$

$K'|K$ d° impa

On peut supposer que A est semi-simple, en fait m algèbre à involution simple:

$$A = A_1 \times \dots \times A_r \times A_{r+1} \times A^*_{r+1} \times \dots \times A_s \times A^*_s$$

[Certaines sont invariantes par involution $A_i = A_i^\times$
D'autres échangées

$$H^1(K, U_A) = H^1(K, A_1) \times \dots \times H^1(K, U_{A_r})$$
$$\times \underbrace{H^1(K, U_{A_{r+1} \times A^*_{r+1}})}_{\overset{\shortparallel}{0.}} \times \dots \times \underbrace{H^1(K, \cancel{A_{r+1}} \times U_{A_{s+1} \times A^*_{s+1}})}_{\overset{\shortparallel}{0.}}$$

$U_{B \times B^\times} = Gl_B$ et "Hilbert 90".

Reste à démontrer ce qu'on veut pour A une K-algèbre à involution simple.

Thme (Bak, 1969): Si N_1 et N_2 sont des modules hermitiens, tels que

$$N_1 \oplus H(A) \cong N_2 \oplus H(A)$$

H(A) plan hyperbolique sur A.

$= Ax \oplus Ay$ muni de $\langle x, x\rangle = \langle y, y\rangle = 0$. $\langle x, y\rangle = 1$

Alors $N_1 \cong N_2$

Rques: $\langle\ ,\ \rangle = h$ ds la notation antérieure
On suppose ts les mod hermitiens non dégénérés (vrai ss cela aux

On appelle (x,y) paire hyperbolique

<u>Remarque</u>: Ceci entraîne que

$$N_1 \oplus N \cong N_2 \oplus N \Rightarrow N_1 \cong N_2$$

Il suffit d'ajouter "$-N$" de chaque côté:

$$N \oplus -N \cong H(N).$$

Il existe M tq $N \oplus M \cong A^n$

d'où $N_1 \oplus H(A)^n \cong N_2 \oplus H(A)^n$

et par récurrence se déduit du thme énoncé.

Réf: B. Keller <u>Math</u>. <u>Zeit</u>. 198 1988.

M. Knus livre à paraître chez Springer.

(Quebbemann, R. Scharlau, W. Scharlau, Schulte, Mémoires SMF ~ 1976 très général)

<u>Démonstration</u>

$M = N \oplus H(A)$ forme hermitienne $\langle\,,\,\rangle$

(x,y) paire hyperbolique

<u>Lemme</u> $U(M)$ <u>agit transitivement sur l'ensemble des plans hyperboliques de</u> M.

lemme $\Rightarrow$ théorème

$$M = N_1 \oplus H_1 = N_2 \oplus H_2$$

$\varphi : M \to M$ $\quad \varphi(H_1) = H_2$, alors $\varphi(\underset{\overset{\shortparallel}{N_1}}{H_1^\perp}) = \underset{\overset{\shortparallel}{N_2}}{H_2^\perp}$.

Transvections $(M, \langle\ \rangle)$

Soient
$$\left|\begin{array}{ll} u \in M & \langle u, u\rangle = 0. \\ v \in M & \langle u, v\rangle = 0. \\ a \in A & \text{tel que } a + \bar{a} = \langle v, v\rangle. \end{array}\right.$$

Posons : $\sigma_{u,a,v}(x) = x + \langle x, v\rangle u - \langle x, u\rangle v - \langle x, u\rangle a$

Lemme : 1) C'est une isométrie : $\sigma_{u,a,v} \in U(M)$.

2) $\varphi\, \sigma_{u,a,v}\, \varphi^{-1} = \sigma_{\varphi(u), a, \varphi(v)}$ pour tout $\varphi \in U(M)$.

3) $\sigma_{u,a',v'} \circ \sigma_{u,a,v} = \sigma_{u, a+a'+\langle v, v'\rangle, v+v'}$

Vérification par calcul direct.

Isométries hyperboliques

$M = N \oplus H$

isométrie de H étendue à M par identité

$H = H(A)$ avec paire hyperbolique x, y

$\alpha \in A^*$ $\quad H_{x,y}(\alpha) \in U(H) \subset U(M)$

$$H_{x,y}(\alpha)(x) = \alpha x$$
$$H_{x,y}(\alpha)(y) = \bar{\alpha}^{-1} y$$

On note $G(M, x, y)$ le sous-groupe de $U(M)$ engendré par les transvections $\sigma_{u,a,v}$ avec $u \in Ax \cup Ay$ $\quad v \in N$ et par les $H_{x,y}(\alpha)$, $\alpha \in A^{\times}$.

Proposition : $G(M, x, y)$ agit transitivement sur les paires hyperboliques ($N \neq 0$ ici).

Proposition Soit (x', y') une autre paire hyperbolique de M, avec :

$$x' = \alpha x + \beta y + u \qquad u \in N$$

Si $\alpha \in A^\times$ alors il existe $\varphi \in G(M, x, y)$ tq

$$\varphi(x) = x' \text{ et } \varphi(y) = y'.$$

Démonstration

$$0 = \langle x', x' \rangle = \alpha \bar{\beta} + \beta \bar{\alpha} + \langle u, u \rangle$$

d'où $\langle u, u \rangle = -\alpha\bar{\beta} - \beta\bar{\alpha}$.

$$\langle \alpha^{-1} u, \alpha^{-1} u \rangle = -\bar{\beta}\,\bar{\alpha}^{-1} - \alpha^{-1}\beta$$

$$\sigma_{y, -\alpha^{-1}\beta, -\alpha^{-1}u} \in G(M, x, y)$$

$$\sigma_{y, -\alpha^{-1}\beta, -\alpha^{-1}u}(x) = \alpha^{-1} x'$$

$$\psi = H_{x,y}(\alpha) \circ \sigma_{y, -\alpha^{-1}\beta, -\alpha^{-1}u}$$

$$\psi^{-1}(y') = \gamma x + \delta y + v$$

$$\langle \psi^{-1}(x'), \psi^{-1}(y') \rangle = 1 = \langle x, \gamma x + \delta y + v \rangle$$
$$= \delta$$

$$\langle v, v \rangle = -\gamma - \bar{\gamma}$$

$$\sigma_{x, -\gamma, -v}(x) = x$$

$$\sigma_{x, -\gamma, -v}(y) = \psi^{-1}(y').$$

Posons $\varphi = \psi \circ \sigma_{x,-\gamma,-v}$

On a : $\varphi(x) = x'$

$\varphi(y) = y'$.

Remarque. Soit $z \in N$, $\langle z, z\rangle = \rho + \bar{\rho}$

$\sigma_{x,\rho,z}(x') = (\alpha - \beta\rho + \langle u, z\rangle)x + \ldots$

Donc il suffit de trouver un z dans N

tq $\begin{cases} (\alpha - \beta\rho + \langle u, z\rangle) \text{ soit inversible.} \\ \langle z, z\rangle = \rho + \bar{\rho} \end{cases}$

- Corps gauches $A = D$.

Soit (x', y') une "autre paire".

$x' = \alpha x + \beta y + u$

Si $\alpha \neq 0$ OK.

Sinon il faut trouver $z \in N$ $\langle u, z\rangle - \beta\rho \neq 0$.

si $u \neq 0$ on peut trouver $z \in N$ tq (u, z) soit une paire hyperbolique

si $u = 0$ OK aussi avec $z \neq 0$.

Soit M un module hermitien, $M \neq H(A)^n$.

Soient $(x_1, y_1), \ldots, (x_n, y_n)$ des paires hyperboliques orthogonales deux à deux.

Soit $G \subset U(M)$ engendré par les $G(M, x_i, y_i)$

Lemme G agit transitivement sur l'ensemble des n-uples de paires hyperboliques orthogonales deux à deux.

Démonst. par récurrence

Algèbres simples

Soit D un corps gauche muni d'une involution $D \to D$

$A = M_n(D)$ et soit $*$ $A \to A$ involution donnée par $(d_{ij})^* = (\overline{d}_{ji})$.

Soient $e_{ij} = \begin{pmatrix} 0 & 0 \\ & 1 \\ 0 & 0 \end{pmatrix}$

$e_{11} =: e$ Soit $M = N \oplus H$ un module hermitien et (x, y) une paire hyperbolique de H $(\cong H(A))$

Proposition 1) $(eM, <,>_{|eM})$ est un module hermitien sur $D = eAe$

2) eH est la somme $\perp$ de n plans hyperboliques $H_i \cong H(D)$ avec paire hyperbolique $(e_{1i}x, e_{1i}y)$.

3) Tout élément de $U(eM)$ s'étend de façon unique en un élément de $U(M)$.

Rque: $e = e_{11}$ est bien un projecteur hermitien.

Théorème

1) $G(eM, e_{1i}x, e_{1i}y) \subset G(M, x, y)$

2) $G(M, x, y)$ agit transitivement sur l'ensemble des paires hyperboliques.

Démonstration

Montrons que les extensions des générateurs sont dans $G(M, x, y)$.

- Clair pour ceux de la forme $H(\alpha)$
- $\sigma_{z,a,u}$ une transvection associée à H_i plan hyperbolique engendré par $e_{1i}x$, $e_{1i}y$

$z = e_{1i}x$ ou $e_{1i}y$ ou multiple

et $u \in H_i^{\perp}$.

Si $u \in H^{\perp} = N$ $\sigma_{z,a,u} \in G(M, x, y)$

Sinon soit $u = v + w$ avec $v \in H$

$w \in H^{\perp} = N$

$\sigma_{z,a,u} = \sigma_{z,b,v} \circ \sigma_{z,c,w}$ $\left| \begin{array}{l} b + b^* = \langle v, v \rangle \\ c + c^* = \langle w, w \rangle \end{array} \right.$

$\sigma_{z,c,w} \in G(M, x, y)$

$\sigma_{z,b,v}(x) = \alpha' x + \beta' y$ On voit que $\alpha' \in A^{\times}$.

Il existe par la proposition du début un

$\varphi \in U(H)$ avec $\varphi(x) = x'$ $\varphi(y) = y'$

$\varphi \in G(H, x, y)$ donc $\varphi = \sigma_{z,b,v}$

Reste le cas où l'involution ~ est quelconque
Il existe une unité $c \in A^\times$ telle que
$\tilde{x} = c x^* c^{-1}$

On peut choisir c tel que $c^* = \pm c$

Proposition. Soit $(M, <,>)$ un module hermitien sur $(A, \sim)$. Alors

1) $(M, <,>c)$ est un module hermitien sur $(A, *)$

2) Soit (x, y) une paire hyperbolique de $(M, <,>)$. Alors $(x, c^{-1}y)$ est une paire hyperbolique pour $(M, <,>c)$.

3) Les sous-groupes du groupe unitaire se correspondent

$$G(M, <,>, x, y) = G(M, <, >c, x, c^{-1}y).$$

Serre 8 avril 1991

176

G - formes quadratiques

G groupe fini, K corps car $\neq 2$

V espace vectoriel de dim finie n sur K

muni d'une action de G

forme quadratique $q : V \to K$ non dégénérée

invariante par G.

Ex 1 : L/K ext. gal. de groupe G

q_L forme trace sur L

(L, q_L) action de G

Plus généralement, L peut être une G-algèbre

galoisienne sur K

Exemple 2 V base $(e_g)_{g \in G}$,

$g e_h = e_{gh}$ (à gauche)

q forme quadratique telle que e_g base

orthonormale.

$$q(e_g, e_{g'}) = \begin{cases} 0 & g \neq g' \\ 1 & g = g' \end{cases}$$

"G - forme quadratique unité"

il existe un vecteur $e \in V$ tel que

ge $(g \in G)$ base de V

$$q(e, ge) \begin{array}{ll} = 0 & \text{si } g \neq 1 \\ = 1 & \text{si } g = 1 \end{array}$$

L/K a une base normale autoduale (BNA)

"belle base"

Si $(L, q_L,$ action de $G) \simeq G$-forme quadratique unité

$\Longleftrightarrow$ il existe $e \in L$, tel que :

(ge) base de L

$$Tr(e.ge) = \begin{cases} 0 & si\ g \neq 1 \\ 1 & si\ g \neq 1 \end{cases}$$

Il n'est pas commode de rester dans le cadre des extensions de corps.

<u>"G-algèbre galoisienne"</u>

$n \geq 1$; K corps de base, G groupe fini, $|G| = n$

Une K-algèbre commutative L munie d'une action de G

<u>Conditions</u> équivalentes

(1) Après extension des scalaires, L devient isomorphe à $K \times \dots \times K$ (n copies) avec action simplement transitive de G

$L \simeq \prod_G K$ sur ext. convenable (si une telle extension existe, on peut la supposer séparable).

(2) L est l'algèbre affine d'un G-<u>torseur</u> sur K (espace principal homogène à droite sur G)

[L sert à tordre des objets où opère G.]

(3) L est une K-algèbre étale de rang n, et l'action de G sur $\Omega(L) = \mathrm{Hom}^{alg}(L, K_s)$, K_s clôture séparable, est simplement transitive.

$\Omega(L)$: ensemble à n éléments, avec action de $G_K = \mathrm{Gal}(K_s/K)$ à gauche, action à droite de G (s. trans.), commutant à la précédente.

(4) L est étale, et la représentation de G dans L est isomorphe à la représentation régulière.

Alors :

(5) L est un produit de corps, extensions galoisiennes de degré fini de K, permutés par G.

Réclame :

(1) ext. des scalaires L/K G-gal
K'/K ext, $L \otimes_K K'$ G-alg. gal.

(2) Induction :
Si $\varphi : G \to G'$ est un homomorphisme de groupes finis, toute G-algèbre galoisienne définit une G'-algèbre galoisienne induite L'

$L' \to L$ compatible avec l'action de G

Le couple formé de
L' et $L' \to L$ sont déterminés à isom. unique

$H \subset G$, alg. ind : $\mathrm{Ind}_H^G(K_H)$

Pour toute G-algèbre galoisienne, il existe un s/g H de G (défini à conj. près) et une ext. gal. K_H de K à groupe de Galois H, telle que $L = \mathrm{Ind}_H^G(K_H)$.

Classes d'isom. de G-alg. gal. $\longleftrightarrow$ repr. gal. dans G hom. (à conj. près) $\rho : G_K \to G$

Opérations de changement de base ① et ② :

① K'/K $\quad G_{K'} \to G_K \to G$

② Induction $\quad G_K \to G \to G'$

Question :

Peut-on donner un critère pour l'existence d'une "belle base" pour G-alg. gal. L ?

Plus généralement :

G-forme quadratique $\overset{?}{=}$ forme unité ?

Condition nécessaire :

(V, q) repr. de G ds $V \simeq$ repr. régulière (*

Lemme :

Si K est algébriquement clos, $(*) \Longleftrightarrow$ forme unité.

$e \in V$, $q(e, ge) = 0$ $g \in G$, $g \neq 1$

$q(e,e) = 1$.

~~forme quadratique $q_g(x) = q(x, gx)$ $n-1$ formes $n-1 < n$, donc $\exists e \neq 0$, $e \in V$ comme ci-dessus.~~ (Se démontre avec les formes hermitiennes)

$q(e,e) \neq 0$

G - formes quadratiques qui sont des "K-formes" de la G - forme unité.

Automorphismes de la G - forme unité

Groupe unitaire U_A de l'algèbre à involution $A = K[G]$, munie de l'involution $g^* = g^{-1}$

$\sum a_g\, g \longmapsto \sum a_g\, g^{-1}$.

V base (ge) $e \in V$

Automorphisme $u : e \mapsto \sum a_g\, ge$

u respecte la forme quadratique $\Longleftrightarrow$

$(\sum a_g\, g)^* (\sum a_g\, g) = 1$, i.e. $u^* u = 1$.

Conclusion:

~~toute~~ Une telle G - forme quadratique s'obtient de la G - forme unité par torsion au moyen d'un élément de $H^1(K, U_G)$

U_G : groupe unitaire de $K[G]$.

Cas particulier :

G-forme est celle attachée à une G-algèbre galoisienne L/K.

G-algèbre galoisienne L correspond à un homomorphisme $\rho : G_K \to G$.

$$\begin{tikzcd} G_K \arrow[r] \arrow[rr, bend right, "1\text{-cocycle}"'] & G \arrow[r] & U_G(K) \end{tikzcd}$$

La classe de cohomologie $u_L \in H^1(K, U_L)$ attachée à L est la classe du cocycle $G_K \to G \to U_G(K)$.

Théorème (BL)

Deux G-formes quadratiques qui deviennent isomorphes après extension de degré impair du corps K, sont isomorphes.

G-forme quadratique : cas particulier d'un tenseur de degré 2

V, q, $g \in G$

$V^* \otimes V^*$ $\quad V \otimes V^*$

Corollaire 1 :

Si : L est une G-algèbre galoisienne, et si : $L \otimes_K K'$ a une belle base avec $[K':K]$ impair, alors L a une belle base.

On pourra donc supposer :

1. K parfait
2. G_K est un pro-2-groupe.

Corollaire 2 :

Si : G est d'ordre impair, alors L a une belle base.

Propriété des algèbres galoisiennes ayant une belle base :

L une G-algèbre galoisienne.

X "objet" = espace vectoriel muni de tenseurs v.

$L \longleftrightarrow P$ "torseur" $(= \operatorname{Spec} L)$

X_P : tordu de X par P

Donnée de L : $G_K \to G$

On a un 1-cocycle $G_K \to G \to \operatorname{Aut}(X)$

Th : Si L a une belle base, et si les tenseurs sont de degré 2, alors $X_P \simeq X$.

$V, v_\alpha \longrightarrow$ algèbre à involution R

$$U_R = \mathrm{Aut}(V, v_\alpha)$$

$$G \longrightarrow U_R(K) \subset R$$

$K[G] \longrightarrow R$ compatible à l'involution

$$U_G \longrightarrow U_R$$

le cocycle u_L étant trivial, son image dans U_R aussi.

Groupes d'ordre pair :

Remarque : Si $K = \mathbb{R}$ (ou plus généralement corps ordonné maximal), une G-algèbre galoisienne est caractérisée par un élément $s \in G$ (à conj. près) tel que $s^2 = 1$

$G_K \to G$ trivial ou inv.

belle base existe $\Longleftrightarrow$ $s = 1$.

$s \neq 1$, forme trace de L a des signes $+$ et $-$,

en fait $\cong \langle \underbrace{1, \dots, 1}_{n/2}, \underbrace{-1, \dots, -1}_{n/2} \rangle$

$(L \simeq \underbrace{\mathbb{C} \times \dots \times \mathbb{C}}_{n/2})$

$s = 1 \Longleftrightarrow L$ est (totalement) réel

Remarque :

Si l'ordre de G est pair, alors il existe (sur $\mathbb{R}$) des G-algèbres galoisiennes sans belle base.

Théorème :

Supposons que $cd_2 K \leq 1$. Soit L/K une G-algèbre galoisienne. Pour que L ait une belle base, il faut et il suffit que les conditions équivalentes (1), (2) ci-dessous soient satisfaites :

(1) Image de $G_K \to G$ est contenue dans tout s/g d'indice 2 de G

(2) Pour tout $z \in H^1(G, \mathbb{Z}/2\mathbb{Z})$, on a $z_L = 0$ dans $H^1(K, \mathbb{Z}/2\mathbb{Z})$.

Lemme (vrai pour tout corps K)

1. Si L/K a une belle base, et si H est un s/g de G, la forme trace de L^H est la forme unité

2. Pas vrai pour les autres sous-algèbres de L : "théorie de Galois ne s'applique pas" (il y a beaucoup plus de sous-alg. que de sous-groupes).

Démonstration :

Si $(g e)$ est une belle base de L

$$e' = \sum_{h\in H} he \quad , \quad e' \in L^H$$

$$e'g = \sum_{h\in H} hge \qquad e'g \in L^H$$

On vérifie que $Tr_{L^H}(e'_s \cdot e'_t) = \begin{cases} 0 & s \neq t \\ 1 & s = t \end{cases}$

grâce à la formule :

$$Tr_{L^H}\left(\sum_{h\in H} hx \cdot y\right) = Tr_L(xy) \qquad x\in L,\ y \in L^H$$

Autre démonstration :

forme trace de L^H : forme unité de rang $|G/H|$ tordue par l'action de G_A sur G/H, via G.

Or L "ne tord pas les tenseurs quadratiques".

(2) Si L/K a une belle base, et si $H \subset G$ est d'indice 2, alors l'image de G_K dans G est contenue dans H.

L^H extension quadratique de K

forme trace unité

$K(\sqrt{d})$ $\qquad \langle 2, 2d\rangle \qquad$ discr $= d$

forme trace unité $\Longleftrightarrow$ $d = 1$, décomposée

A montrer :

Si (1) est satisfaite, il existe une belle base.

On peut supposer que K est parfait, et que G_K est un pro-2-groupe

$\Downarrow$

K est un corps de dim ≤ 1 (groupe de Brauer de toute ext. gal. de K est 0).

Thm (Steinberg) :
Si K est parfait, de dim ≤ 1, alors $H^1(K, B) = 0$ pour tout groupe algébrique linéaire connexe B

$B = U_G^\circ$: composante connexe de 1 dans U_G.

Lemme :
Le quotient U_G/U_G° est de type $(2, \ldots, 2)$ (avec action de G_K).
(Vrai : pour tout groupe unitaire).

Liste des facteurs / clôture alg.

GL_n, Sp_{2n}, O_n

connexes, sauf O_n. O_n/SO_n de type $(2, \ldots, 2)$.

$$\begin{tikzcd} G \arrow[r] \arrow[dr] & U_G(K) \\ & U_G^0(K) \arrow[u] \end{tikzcd}$$

$u_L \in H^1(K, U_G)$

provient de $\hat{u}_L \in H^1(K, U_G^0)$, on a $u_L^0 = 0$

par Steinberg.

Variante :

Lemme (Bruxelles, 62)

Soit K'/K une extension quadratique de corps parfaits. Soit B réductif connexe.

Soit $z \in H^1(K, B)$ donnant 0 dans $H^1(K', B)$.

Alors il existe un tore maximal T de $B/_K$ et $t \in H^1(K, T)$ donnant z.

$\zeta \in B(K')$, $\zeta\bar{\zeta} = 1$ ($\bar{\ }$: élé non triv. de K'/K)

$\zeta \mapsto g^{-1}\zeta\bar{g}$, $g \in B(K')$

On peut choisir ζ semi-simple régulier (condition ouverte). D'où un unique tore maximal $T/_{K'}$ contenant ζ. Mais $\bar{\zeta} \in T$ aussi

En fait, $T/_K$. ζ définit $t \in H^1(K, T)$

Parenthèse sur la structure de U_G

Hypothèse : car $K = 0$

K assez grand pour que les repr. irréd. de G soient définies sur K

(par ex. K contenant les racines $n^{\text{ièmes}}$ de 1, $n = |G|$).

$$K[G] = \prod_{\chi \text{ car irréd.}} M_\chi$$

- $\chi = \overline{\chi}$
- $\chi = \overline{\chi}$ $\begin{cases} \text{repr. orthogonales} \\ \text{repr. symplectiques} \end{cases}$
- $M_\chi \times M_\chi$, involution échange les facteurs

  groupe unitaire : $M_\chi^* \simeq GL_{n_\chi}$

  et son $H^1 = 0$

- Groupe unitaire $= O(q_\chi)$

  H^1 = classes de f.q. de rang n_χ

  G. u $= Sp$, $H^1 = 0$

$$H^1(K, U_G) \simeq \prod_{\substack{\chi \text{ de} \\ \text{type orth.}}} H^1(K, O(q_\chi))$$

Le cas général est plus difficile, car on a des groupes unitaires sur des corps gauches munis d'involutions.

Exemple :

$\boxed{G = A_4}$, $A_4/(2,2) = C_3$ $\quad$ $\overset{1}{\text{conj.}}$ $\mathbb{Q}(\sqrt{-3})$

Supposons d'abord que $\sqrt{-3} \in K$.

$$A_G \simeq K \times \overset{\longleftrightarrow}{K \times K} \times M_3(K).$$

$$U_G \simeq \mu_2 \times G_m \times O_3 \qquad O_3 = O(q_3)$$
$$q_3 = \langle 1,1,1 \rangle.$$

L/K alg. gal. à groupe $G = A_4$

$u_L \in H^1(K, U_G)$

Composante de (u_L) ds μ_2 est 0

$$G_K \longrightarrow G \longrightarrow U_G$$

$$G \longrightarrow 1 \subset \mu_2$$

composante de (u_L) ds G_m est 0

composante de (u_L) ds O_3 $\hookrightarrow$

forme quadratique à 3 variables

$L \to K_4 = L^{A_3}$, alg. étale de

dim 4, discriminant 1

$$q_{K_4} = \langle 1 \rangle \oplus q^0_{K_4}.$$

Si $G = A_4$, il y a équivalence entre :

1 belle base

2 $q^0_{K_4} = \langle 1,1,1 \rangle$

2' $q_{K_4} = \langle 1,1,1,1 \rangle$

3 $G_K \to A_4$ se relève en $G_K \to \tilde{A}_4$.

4 Si $z \in H^2(A_4)$ est l'unique élément non nul, on a $z_L = 0$ dans $H^2(K)$.

Mêmes résultats si $\sqrt{-3} \notin K$:

Au lieu d'un G_m on a un G_m tordu.

La semaine prochaine, on verra comment ça se généralise pour les groupes dont les 2-Sylows sont abéliens élémentaires.

K corps de nombres.

Hypothèse sur G. $H^1(G) = H^2(G) = 0$.

Théorème Sous les hypothèses ci-dessus :
Une G-algèbre galoisienne a une belle base, si et seulement si elle est totalement réelle (par rapport aux places réelles de K).

Cor : Vrai si K est totalement imaginaire

Exemple : G = Monstre.

Corollaire (K corps de nombres)
Th. Soit L une G-algèbre galoisienne sur K,
$G = A_n$, $n \geq 4$.
Alors L a une belle base si et seulement si :

(a) L est totalement réelle

(b) $G_K \to A_n$ se relève en $G_K \to \tilde{A}_n$

On applique le thm à $\tilde{A}_n$.

(a) et (b) $\Rightarrow$ belle base

$\tilde{A}_n$- alg. gal. $\tilde{L}$ (donnant L)

Les conjugaisons complexes c ds $\tilde{A}_n$,

$c^2 = 1$, $c \mapsto 1$ dans A_n.

$c = \begin{cases} 1 \\ -1 \end{cases}$ 'élé' non triv. de $\tilde{A}_n$.

Le relèvement $G_K \to \tilde{A}_n$ peut être modifié par un car. $G_K \to \{\pm 1\}$.

On corrige, et on a $c = 1$ pour toute place.

Alors $\tilde{L}$ a une belle base.

$H = \{1, -1\}$, $L = \tilde{L}^H$; donc L a une belle base.

Inversement:

Si L a une belle base, posons

$K_n = L^{A_{n-1}}$.

La forme trace est $\langle 1, \dots, 1 \rangle$.

Donc $w_2 = 0$. On sait que w_2 est l'obstruction à relever.

Démonstration:

Sous l'hypothèse plus forte que $G = G'$.

Th (M. Kneser):

Soit K un corps de nombres, et soit $\mathcal{B}$ un groupe semi-simple connexe, simplement connexe, Soit $z \in H^1(K, B)$. Alors si $z \mapsto 0$ pour tout plongement réel de K, alors $z = 0$.

(Harder, Cernousov, Premet : cas exeptionnels).

U_G^0 : comp. neutre de U_G
c'est un groupe réductif connexe

U_G^1 : semi-simple connexe
(groupe dérivé de U_G^0).

$$\begin{array}{c} \tilde{U}_G^1 \\ \downarrow \\ U_G^1 \subset U_G^0 \subset U_G \end{array}$$

$u_L \in H^1(G_K, U_G)$, $G_K \to G \to U_G(K)$
plongement évident.

1) On a déjà vu que l'image de G est contenue dans $U_G^0(K)$

2) Comme $G = [G, G]$, image est contenue dans $U_G^1(K)$.

$$\begin{array}{c} \tilde{U}^1_G(K) \\ \pi \downarrow \\ G \subset U^1_G(K) \end{array}$$

③ $G \subset \pi \tilde{U}^1_G(K)$. En effet,

$$1 \to C \to \tilde{U}^1_G \to U^1_G \to 1$$

$$\begin{array}{ccccc} \tilde{U}^1_G(K) & \to & U^1_G(K) & \to & H^1(K, C) \\ & & \uparrow & \nearrow_{\text{hom}} & \\ & & G & & \end{array}$$

C est de type $(2, \dots, 2)$ (avec action de Galois).

Donc $H^1(K, C)$ est abélien annulé par 2

Soit $\tilde{G}$ l'image réciproque

$\tilde{G} = \pi^{-1}(G)$, isom. à $G \times C(K)$

On a supposé $H^2(G) = 0$.

Donc G se relève

$$\begin{array}{ccc} \tilde{G} & \subset & \tilde{U}_G(K) \\ \downarrow\uparrow & & \downarrow \pi \\ G & \subset & U^1_G(K) \end{array}$$

$\tilde{z}_L \in H^1(K, \tilde{U}_G^1)$ est 0 ?

$$G_K \to G$$
$$c \longmapsto 1$$

Un peu plus compliqué quand $G \neq [G, G]$.

Problème ouvert :

Généraliser ceci aux corps parfaits avec $cd_2\, K \leq 2$.

Est-ce qu'il est vrai que si $H^1 = H^2 = 0$, une belle base existe ?

Serait vrai si on savait :

$cd(K) \leq 2 \Rightarrow H^1(K, \underset{\text{connexe}}{\text{semi-simple simplement}}) = 0$

Dans cette direction, on a en tout cas :

Merkurjev - Suslin

$cd \leq 2 \Rightarrow D$ algèbre centrale simple$/K$,

$$K^* = \mathrm{Nrd}\, D^*.$$

Prochaine fois :

2 - Sylow ab. él. $\underbrace{(2, \ldots, 2)}_{r \text{ facteurs}}$

G-algèbre galoisienne avec 2-groupe de Sylow abélien élémentaire.

Enoncé des résultats (Bayer-Serre, en préparation)

K corps de car $\neq 2$, G groupe fini,

S 2-Sylow de G, $N = N_G(S)$

$|G| = 2^r \cdot m$, m impair, $2^r = |S|$

L G-algèbre galoisienne $/K$

Existe-t-il une belle base ?

q_L = forme trace de L, de rang $2^r m$

(1) Th 1 : Il existe une K-forme quadratique q_L°, de rang 2^r, et une seule à isom. près, telle que

$$q_L \simeq m \otimes q_L^\circ \quad (= q_L^\circ \oplus \cdots \oplus q_L^\circ,\ m \text{ fois})$$

Proposition :
Soit f une forme quadratique sur K, et soit K' une extension finie de K de degré impair. Soit m impair ≥ 1.
Si f est divisible par m sur K', f est divisible par m sur K.

Résulte des thm de Springer

$G_k \longrightarrow G$ définissant L/k.

Après extension de degré impair, on peut supposer que $\pi(G_k) \subset S$.

Remarque: Si L a une belle base, alors q_L^0 est la forme unité: $q_L^0 = 2^r \otimes \langle 1 \rangle$.

D'où condition nécessaire pour l'existence d'une belle base.

2) Supposons S abélien élémentaire, de type $(2, \ldots, 2)$, de rang r.

Th 2: La forme q_L^0, multipliée par 2^r, est une r-forme de Pfister.

Autrement dit: si r est pair, q_L^0 est une forme de Pfister, si r est impair, $2q_L^0$ est une forme de Pfister.

Proposition (déjà vu)
Si une forme quadratique devient une forme de Pfister par extension des scalaires, de degré impair, elle l'est déjà.

Th 3 : On fait 2 hypothèses :

(1) S est abélien élémentaire

(2) L'action de N/S sur S par conjugaison est transitive sur $S - \{1\}$.

Il y a alors équivalence entre :

(a) L a une belle base

(b) q_L^0 est la forme unité $\langle 1, \dots, 1\rangle$

(b') $2^r q_L^0$ ——— $\langle 1, \dots, 1\rangle$.

Il est trivial que (a) $\Rightarrow$ (b)

(b) $\Rightarrow$ (b'), car $2\langle 1, \dots, 1\rangle \cong \langle 1, \dots, 1\rangle$
($\langle 2, 2\rangle \cong \langle 1, 1\rangle$).

③ Cohomologie de G

Prop : L'application de restriction

$$H^i(G) \longrightarrow H^i(S)$$

est injective, et son image est formée des éléments de $H^i(S)$ qui sont invariants par l'action de $W = N/S$.

(Résultat vrai chaque fois que le 2-Sylow est abélien et G-module p-primaire (ici $p=2$) à action triviale de G)

Si S est un groupe abélien élémentaire de rang r, alors $H^*(S) = \mathrm{Sym}\, H^1(S)$ = alg. de pol. en r générateurs de d° 1.

Th 4 : Il existe dans $H^r(G)$ un élément z ayant la propriété suivante :

– La restriction de z à tout s/g de G d'ordre 2 est $\neq 0$.

– Cet élément est unique, à l'addition près de classes de cohomologie "négligeables".

L est associé à un homomorphisme $\pi : G_K \to G$. Si $x \in H^i(G)$, $\pi^* x \in H^i(G_K) = H^i(K)$.

Je pose $x_L = \pi^* x \in H^i(K)$.

En particulier, z_L est un élément bien défini de $H^r(K)$, indépendant du choix de L.

Th 5 : L'invariant cohomologique dans $H^r(K)$ de la forme de Pfister $2^r q_L^0$ est $z_L + (-1)\dots(-1) = z_L + e^r$,

$e = (-1) \in H^1(K)$.

r- forme de Pfister :

$\simeq \langle 1, -\alpha_1 \rangle \otimes \cdots \otimes \langle 1, -\alpha_r \rangle = \langle\langle \alpha_1, \dots, \alpha_r \rangle\rangle$.

Son invariant d'Arason est $(\alpha_1) \cdots (\alpha_r) \in H^r(K)$

En particulier, $\langle 1, \dots, 1 \rangle$ a pour invariant cohomologique $(-1) \cdots (-1) = e^r \in H^r(K)$.

Corollaire : La forme $2^r q_L^0$ a même invariant cohomologique que la forme unité si et seulement si $z_L = 0$.

Th 6 : Si $r \leq 4$ (ou si les conjectures de Milnor sont vraies pour le corps K), On suppose W agit transitivement sur $S-\{1\}$

L a une belle base $\Longleftrightarrow z_L = 0$.

Exemples :

$\boxed{r = 0}$ G est d'ordre impair.

Pas de condition — tjs belle base.

$\boxed{r = 1}$ Si $S = C_2$, il existe $G \xrightarrow{z} C_2 \to 1$

$$\begin{array}{c} \nearrow \\ G_K \end{array}$$

$H^1(G) = \mathbb{Z}/2\mathbb{Z}$. $1 \to H \to G \to C_2 \to 1$

$z \in H^1(G)$. On veut $z_L = 0$

belle base $\Longleftrightarrow \pi G_K \subset H$, H d'ordre impair.

$\boxed{r=2}$ $S = (2,2)$

$\mathrm{Aut}\, S = S_3$, image de N/S dans $\mathrm{Aut}\, S$ est soit $\{1\}$ ou $C_3 = A_3$.

Si l'action est transitive, N/S opère par C_3 sur S.

$z \in H^2(G)$ est unique.

x, y base de $H^1(S)$, on a $z = x^2 + xy + y^2 \in H^2(S)$ invariant par N/S.

Il existe une extension centrale non triviale unique

$$1 \longrightarrow C_2 \longrightarrow \tilde{G} \xrightarrow{\varphi} G \to 1$$

de classe de cohomologie z.

Tout élément de G d'ordre 2 a une image réciproque dans $\tilde{G}$ formée d'éléments d'ordre 4

$\varphi^{-1}(S) \cong Q_8$, groupe des quaternions.

Le th 6 dit que L a <u>une belle base si et seulement si</u> $\pi : G_K \to G$ <u>se relève en</u> $\tilde{\pi} : G_K \longrightarrow \tilde{G}$.

Si $G = A_4$ ou A_5, on retrouve que le relèvement à $\tilde{A}_4$, $\tilde{A}_5$ est suffisant pour l'existence d'une belle base.

Si $G = PSL_2(\mathbb{F}_q)$, $q \equiv \pm 3 \pmod 8$, belle base $\Longleftrightarrow$ relèvement possible dans $\tilde{G} = SL_2(\mathbb{F}_q)$.

Un relèvement $\tilde{\pi}$ définit une $\tilde{G}$-algèbre galoisienne $\tilde{L}$.

<u>Th 7</u> : <u>Il existe un choix</u> $\tilde{\pi}$ (non unique en général) <u>tel que</u> $\tilde{L}$ <u>ait une belle base</u>.

$\boxed{r=3}$ deux possibilités pour l'action de $W = N/S$. Si transitive (sur éléments $\neq 1$) elle donne soit un groupe C_7, soit $C_3 \cdot C_7$ (produit semi-direct, avec C_7 normal).

<u>Exemple</u> : $SL_2(\mathbb{F}_8)$, 2-Sylow $S = \mathbb{F}_8$ $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, $N = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, N/S opère par $\mathbb{F}_8^* \simeq C_7$.

Groupe de Janko J_1, N agit par un groupe d'ordre 21.

(Noter que $W = N/S$ est contenu dans $SL_3(\mathbb{F}_2) = G_{168}$, d'ordre impair, et que $168 = 8 \cdot 21$)

On peut décrire z explicitement.

On identifie S à $\mathbb{F}_8$, de sorte que l'action de N soit par homothétie (cas $SL_2(\mathbb{F}_8)$), par homothétie et conjugaison (cas J_1).

$z \in H^3(S)$? Polynôme de d° 3.

On considère $N_{\mathbb{F}_8/\mathbb{F}_2} = N$.

c'est un polynôme cubique, après choix d'une base de $\mathbb{F}_8$ sur $\mathbb{F}_2$.

$N(\lambda t) = N(\lambda) N(t)$, $\quad N(\lambda) = 1$ si $\lambda \in \mathbb{F}_8^*$.

Belle base $\iff z_L = 0$.

<u>Exemples</u> de calcul de z_L.

1. $G = SL_2(\mathbb{F}_8)$.

" Méthode de rigidité " permet de

fabriquer des extensions de $\mathbb{Q}(T)$ à groupe de Galois G, ramifié en 3 points (conjugué par le corps cubique de disc. 9^2), la ramification étant d'ordre 3.

Si K est de car 0, et si $t \in \mathbb{P}_1(K)$, distinct des 3 points de ramification,

$$\Downarrow$$

L_t G-algèbre galoisienne sur K (spéc.)

D'où un invariant $z_{L_t} \in H^3(K)$.

<u>Th</u> : <u>Cet invariant est</u> $(-1)(-1)(-1) = e^3$.

<u>Donc</u> L_t <u>a une belle base</u>

$$\Updownarrow$$

-1 <u>est somme de</u> 4 <u>carrés dans</u> K.

L_T alg. gal. sur $\mathbb{Q}(T)$

Invariant $(-1)(-1)(-1) \in H^3(\mathbb{Q}(T))$.

$z_{L_T} \in H^3(\mathbb{Q}(T))$

J_1 ramification d'ordre $2, 5, 5$

conj. $/\mathbb{Q}(\sqrt{5})$

Invariant : $(-1)(-1)(-1)$.

Action non transitive

$r \leq 3$ facile

$r = 3$, action de W par C_3

$$S = (2,2) \oplus 2$$

C_3 — fixe

Alors $1 \to H \to G \to C_3 \to 1$

Il faut que $\pi(G_k) \subset H$ (où $\pi : G_k \to G$ corr. à L) et que la H-alg. gal. ait une belle base : i.e. $G_k \to H$ se relève en $G_k \to \tilde{H} = 2H$.

$r > 3$ q_L^0 remplacé par " autant de formes quadratiques que d'orbites de W dans $S - \{1\}$ ".

Démonstrations des thm 1 – 6

(1) q_L divisible par m

Vrai après ext. à K', $[K':K]$ impair.

(2) $2^r q_L^\circ$ est de Pfister.

Soit L_S une S-algèbre galoisienne

S de type $(2, \dots, 2)$

S corps, $L_S = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_r})$

L_S a pour base $1, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_r}$

$\sqrt{\alpha_1}\sqrt{\alpha_2}, \dots$

$$q_{L_S} \simeq 2^r \langle 1, \alpha_1, \alpha_2, \dots, \alpha_1\alpha_2 \dots \rangle =$$

$$= 2^r \langle\langle -\alpha_1, \dots, -\alpha_r \rangle\rangle$$

Autre démonstration (plus simple)

$L_S = K(\sqrt{\alpha_1}) \otimes \cdots \otimes K(\sqrt{\alpha_r})$

produit tensoriel de $\langle 2, 2\alpha_i \rangle$.

Th 2 : $2^r q_L^\circ$ est de Pfister

Il suffit de le voir sur K',

$\pi(G_K) \subset S$, L est induite d'une

S-algèbre galoisienne L_S

$$q_L = q_{L_S} \oplus \cdots \oplus q_{L_S} = n \otimes q_{L_S}$$

<u>Th 3</u> : <u>Si</u> W <u>opère transitivement sur</u> $S - \{1\}$,

alors q_L^0 <u>unité</u> $\Longrightarrow$ <u>belle base</u>.

On peut supposer que $L = \mathrm{Ind}_S^G L_S$,

où L_S est une S-algèbre galoisienne.

(quitte à remplacer K par K', [K':K] impair).

$S \subset N \subset G$

$L_N = \mathrm{Ind}_S^N L_S$. On va prouver que

L_N a une belle base.

Principe de la démonstration :

N-forme quadratique q_{L_N}, induite de celle de L_S

L_S est une S-algèbre galoisienne.

$S' = \mathrm{Hom}(S, \{\pm 1\}) \simeq H^1(S)$

d'ordre 2^r

$L_S = \bigoplus L_S^x$, dim $L_S^x = 1$.

$$L_S = L'_S \oplus \bigoplus_{\chi \neq 1} L_S^{\chi}$$

L_S^{χ} correspond à $a(\chi) \in K^*/K^{*2}$

1_χ : $\langle e_\chi, e_\chi \rangle = 1$

$s e_\chi = \chi(s) e_\chi$

L_S a comme S- forme quadratique

$$2^r q_{L_S} = \langle 1 \rangle \oplus \sum_{\chi \neq 1} a(\chi) \, 1_\chi$$

$$\mathrm{Ind}_S^N 2^r q_{L_S} = \mathrm{Ind}_S^N \langle 1 \rangle \oplus \sum_{\chi \neq 1} a(\chi) \, \mathrm{Ind} \, 1_\chi$$

$w \in W = N/S$

$$\mathrm{Ind} \, 1_{w(\chi)} \simeq \mathrm{Ind} \, 1_\chi$$

$$\mathrm{Ind}_S^N 2^r q_{L_S} = \mathrm{Ind}_S^N \langle 1 \rangle \oplus \mathrm{Ind} \, 1_\chi \otimes \sum_{\chi \neq 1} a(\chi)$$

On compare L_S à L_S^{depl}

$$q_L^0 \simeq \sum_{\chi \neq 1} a(\chi)$$

Th 4 : Cohomologie

$$H^i(G,A)_p \hookrightarrow H^i(S,A)_p^{N/S} = H^i(S,A)^{N/S}$$

($i \geq 1$ ou coh. de Tate)

A est un G-module

"p" : composante p-primaire

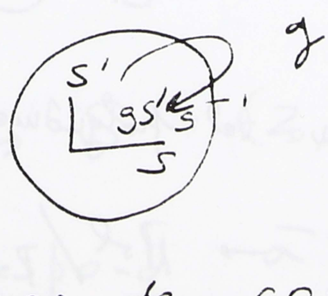
Thm : Si S est abélien et si l'action de G sur A est triviale, alors

$$H^i(G,A)_p = H^i(S,A)^{N/S}$$

Cartan - Eilenberg

"classe de cohomologie stable"

z est stable si, pour tout s/g S' de S et tout $g \in G$, $gS'g^{-1} \subset S$



les classes de cohomologie de $H^i(S',A)$ obtenues à partir de z par les 2 moyens évidents : $\begin{cases} \text{restriction à } S' \\ \text{restriction à } S' \text{ suivie de conjugaison} \end{cases}$

sont égales.

Quand les Sylows sont abéliens, on peut supposer $g \in N$ (lemme de Burnside facile).

<u>Th 4</u> : <u>Il existe</u> $z \in H^r(G)$ qui ne <u>donne</u> 0 <u>dans aucun s/g d'ordre 2 de</u> G.

$H^i(S)$: polynômes homogènes de d° i en r variables.

A fabriquer : polynôme homogène en r variables $f(X_1, \dots, X_r)$ tel que $f(x_1, \dots, x_r) = 1$ pour tout $(x_1, \dots, x_r) \in \mathbb{F}_2^r - \{0\}$.

Ensuite, on le veut invariant par l'action de $W = N/S$.

La Norme $(\mathbb{F}_{2^r} \to \mathbb{F}_2)$ donne un tel polynôme, soit p.

$$0 \to \text{Pol négl} \to \text{Pol} \to \text{Pol}/\text{Pol négl} \to 0$$

Pol négl : pol. dont toutes les valeurs sur $\mathbb{F}_2^r$ sont 0.

(Idéal des pol. négl. est engendré par les polynômes $X_i X_j (X_i + X_j) = X_i^2 X_j + X_i X_j^2$)

$f \in Pol / Pol\, nég$. invariant par W

W est d'ordre impair

Donc f est image d'un polynôme

invariant.

Variante: $\sum_{w \in W} w(f)$!

<u>Th 5</u> : <u>L'invariant d'Arason de $2^r q_L^0$</u> est

$z_L + (-1) \cdots (-1)$.

Il suffit de le voir sur K', auquel cas

$q_L^0 = q_{L_S}$. On est ramené au groupe S

$L_S = \bigoplus L_S^x$

$\pi : G_K \to S = (2, \ldots, 2)$

π correspond à $x_1, \ldots, x_r \in H^1(K)$

Invariant d'Arason cherché est

$(-x_1) \ldots (-x_r) \in H^r(K)$

D'autre part, calculer l'image de t

$$(-x_1)\cdots(-x_r) = \prod (e + (x_i)) \qquad e = (-1)$$

$$= e^r + \sum_{i=1}^{r} e^i \sum_{\gamma_1 < \cdots < \gamma_i} (x_{\gamma_1}) \cdots (x_{\gamma_i})$$

On peut prendre pour f ...

$$f = \sum_{i=1}^{r} \sum_{\gamma_1 < \cdots < \gamma_i} (x_{\gamma_1})^{r-i+1} (x_{\gamma_2}) \cdots (x_{\gamma_i}).$$

$$(\bmod 2,\ x^m = x \quad m \geq 1).$$

$$\pi^*(x)^m = (-1)\cdots(-1)(x) = e^{m-1}(x)$$

car $(x)(x) = (-1)(x) = ex$

Donc l'invariant est $e^r + \pi^*(f)$

<u>Th 7</u> $r = 2$ W agit par $\mathfrak{S}_3$

$$1 \to C_2 \to \tilde{G} \to G \to 1$$

belle base pour L $\iff$ π relevable ds $\tilde{G}$

D'où un $\tilde{L}$.

Le 2-s/g de Sylow est Q_8.

<u>Proposition</u> : <u>La forme</u> $\mathring{q}_{\tilde{L}}$ (de rang 8) <u>est une</u> <u>3-forme de Pfister de type</u> $\langle\langle -1, -1, -\alpha \rangle\rangle$.

(i.e. $\langle 1, 1, 1, 1, \alpha, \alpha, \alpha, \alpha \rangle$).

On étend les scalaires à K' de façon que $\tilde{\pi}(G_K) \subset \tilde{S}$.

$M = M^+ \oplus M^-$ inv. de l'élé central d'ordre 2

anti-invariants

$M^+ \to \langle 1, \dots, 1 \rangle$, $M^- \to \langle \alpha, \dots, \alpha \rangle$.

Descente à K : déc. préservée.

<u>Proposition</u>

<u>belle base</u> <u>pour</u> $\tilde{L}$ $\iff$ $\mathring{q}_{\tilde{L}} \simeq \langle 1, \dots, 1 \rangle$

$\iff$ α <u>est une somme de</u> 4 <u>carrés</u>

$\iff$ $\underbrace{(-1)(-1)(\alpha)}_{u} = 0$ <u>dans</u> $H^3(K)$.

$\tilde{\Sigma} \longmapsto u = (-1)(-1)(\alpha) \in H^3(K)$

On peut modifier $\tilde{\Sigma}$ par $G_K \to (\pm 1)$

$x \in H^1(K)$.

Modification par $x \in H^1(K)$ change

$(-1)(-1)(\alpha)$ en $(-1)(-1)(\alpha x)$

On prend $x = \alpha$: obstruction devient 0.

mod $\boxed{4}$

Fin du cours
