

COURS DE JEAN-PIERRE SERRE

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_>](http://www.numdam.org/item?id=CJPS_1991__12_)

© Bibliothèque de l'IHP, 2015, tous droits réservés.

L'accès aux archives de la collection « Cours de Jean-Pierre Serre » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Notes numérisées par l'IHP et diffusées par le programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/*

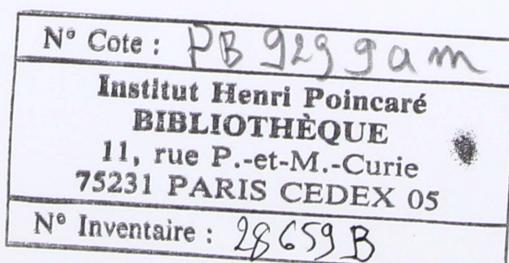
- 4 FEV. 2000

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 du cours 1990-1991

Algèbre et géométrie

- 4 FEV. 2000

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

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

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

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

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

et

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

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

§2. Le cas orthogonal

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

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

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

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

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

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

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

Si m est un entier ≥ 0 , on définit un élément $w_m(q)$ de $H^m(k, \mathbb{Z}/2\mathbb{Z})$ 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 $H^1(k, \mathbb{Z}/2\mathbb{Z})$ défini par $a \in k^*$; le produit $(a_{i_1}) \dots (a_{i_m})$ est un cup-produit dans l'algèbre de cohomologie $H^*(k, \mathbb{Z}/2\mathbb{Z})$.)

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

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

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

2) La même méthode conduit à d'autres invariants. Ainsi, si n est pair ≥ 4 et si $q = \langle a_1, \dots, a_n \rangle$ 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 $H^{n-1}(k, \mathbb{Z}/2\mathbb{Z})$ 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 $x \in H^1(k, O(q))$. On associe à x des éléments

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

de la façon suivante :

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

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

$$1 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \tilde{O}(q) \rightarrow O(q) \rightarrow 1.$$

(Le groupe $\tilde{O}(q)$ est un certain revêtement quadratique de $O(q)$ qui prolonge le revêtement spinoriel $Spin(q) \rightarrow SO(q)$. 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 $\tilde{O}(q)$ 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 :

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

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

2.3. Les conjectures de Milnor

Soit $k^M(k) = \bigoplus k_n^M(k)$ l'anneau de Milnor (mod 2) de k , défini au moyen de symboles multilinéaires $(a_1, \dots, a_n) = (a_1) \dots (a_n)$, $a_i \in k^*$, 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 $W_k \rightarrow \mathbb{Z}/2\mathbb{Z}$.

On définit de façon naturelle des homomorphismes

$$(2.3.1) \quad k_n^M(k) \rightarrow I_k^n/I_k^{n+1}$$

et

$$(2.3.2) \quad k_n^M(k) \rightarrow H^n(k, \mathbb{Z}/2\mathbb{Z}).$$

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 $n \geq 4$.

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

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

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 :

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

On a ainsi défini une application canonique

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

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 $G \rightarrow O(q)$. Vu les hypothèses faites sur G , cet homomorphisme se relève en un homomorphisme $\tilde{\rho} : G \rightarrow \mathbf{Spin}(q)$.

En utilisant (3.1.2) on déduit de là une application

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

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

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

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 ≥ 3) mod 2, mod 3 et mod 5 (car 2,3,5 sont les *nombres premiers de torsion* de E_8 , cf. A. Borel, *Oe. II*, p. 776). J'ignore comment ces invariants pourraient être définis ; je ne sais même pas si les applications $i_p : H^1(k, E_8) \rightarrow H^3(k, \mathbf{Z}/2\mathbf{Z})$ 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

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

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

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 $H^1(k, O(q_1)) \rightarrow H^1(k, O(q))$ 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 $H^1(k, \mathbf{O}(q)) \rightarrow H^1(k', \mathbf{O}(q))$ 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 $H^1(k, \mathbf{O}(q)) \rightarrow H^1(k, \mathbf{O}(q \otimes q'))$ lorsque le rang de q' est impair (le morphisme $\mathbf{O}(q) \rightarrow \mathbf{O}(q \otimes q')$ 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 $H^1(k, F_4) \rightarrow H^1(k', F_4)$ 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 image 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 $\text{Tr}(x^2)$ 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

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

Notons q_A° la forme trace associée à l'algèbre de matrices $M_n(k)$ de même rang que A ; c'est la somme directe d'une forme hyperbolique de rang $n(n-1)$ et d'une forme unité $\langle 1, 1, \dots, 1 \rangle$ 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 $\text{Br}_2(k) = H^2(k, \mathbb{Z}/2\mathbb{Z})$. On a :

$$w_1(q_A) = w_1(q_A^\circ) \quad \text{et} \quad w_2(q_A) = w_2(q_A^\circ) + a.$$

(La formule relative à w_1 est facile. Celle relative à w_2 s'obtient en considérant l'homomorphisme $\text{PGL}_n \rightarrow \text{SO}_{n^2}$ donné par la représentation adjointe et en montrant, par un calcul de poids et racines, que cet homomorphisme ne se relève pas au groupe 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 $e : \text{Gal}(k/k) \rightarrow S_6$ 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 $e' : \text{Gal}(k/k) \rightarrow S_6$ qui correspond à une autre algèbre étale E' de rang 6 (« résolvante sextique »). *Peut-on déterminer $q_{E'}$, à partir de q_E ?* C'est vrai lorsque $w_1(q_E) = 0$, autrement dit lorsque les images de e et e' sont contenues dans le groupe alterné A_6 ; on peut en effet prouver que l'on a dans ce cas $q_{E'} = 2q_E$ (mais pas $q_{E'} \simeq q_E$ en général, bien que q_E et $q_{E'}$ aient les mêmes invariants w_1 et w_2). Lorsque l'on a à la fois $w_1(q_E) = 0$ et $w_2(q_E) = 0$, on peut se demander si q_E est isomorphe à la forme unité $(1, 1, \dots, 1)$. C'est vrai si k est un corps de nombres (ou un corps de fonctions rationnelles sur un corps de nombres) ; c'est faux en général : on peut construire un contre-exemple.

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

Soit G un groupe fini. On s'intéresse aux G -algèbres galoisiennes sur k , ou, ce qui revient au même, aux G -torseurs sur k , G étant considéré comme un groupe algébrique de dimension 0 sur k . Une telle algèbre L est déterminée, à isomorphisme (non unique) près, par la donnée d'un homomorphisme continu $\varphi_L : \text{Gal}(k/k) \rightarrow G$, 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 $\text{Gal}(k_s/k) \rightarrow U_G(k)$, homomorphisme que l'on peut regarder comme un 1-cocycle de $\text{Gal}(k_s/k)$ 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 $\varphi_L : \text{Gal}(k_s/k) \rightarrow G$ l'homomorphisme correspondant. Si x est un élément de $H^n(G, \mathbb{Z}/2\mathbb{Z})$, son image par $\varphi_L^* : H^n(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^n(\text{Gal}(k_s/k), \mathbb{Z}/2\mathbb{Z}) = H^n(k, \mathbb{Z}/2\mathbb{Z})$ sera notée x_L .

(6.3) - *Pour que L ait une BNA, il faut que $x_L = 0$ pour tout élément x de $H^1(G, \mathbb{Z}/2\mathbb{Z})$ (autrement dit, l'image de $\text{Gal}(k_s/k)$ 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 $\text{Gal}(k_s/k)$ est ≤ 1 (autrement dit si les 2-sous-groupes de Sylow de $\text{Gal}(k_s/k)$ 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 $H^1(G, \mathbb{Z}/2\mathbb{Z}) = H^2(G, \mathbb{Z}/2\mathbb{Z}) = 0$.*

(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 , $r \geq 1$; l'ordre de G est $2^m m$, avec m impair.

(6.5.1) - Il existe une r -forme de Pfister q_L^1 , et une seule à isomorphisme près, telle que $2'q_L = m \otimes q_L^1$ (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 $2'm$.
- (iii) La forme q_L^1 est isomorphe à la forme unité de rang $2'$.

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 $H^r(G, \mathbb{Z}/2\mathbb{Z})$ 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 $H^r(k, \mathbb{Z}/2\mathbb{Z})$ est un invariant de l'algèbre galoisienne L .

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

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

L'hypothèse $r \leq 4$ 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 $\text{PSL}_2(\mathbf{F}_q)$ avec $q \equiv 3 \pmod{8}$. Le groupe $H^2(G, \mathbb{Z}/2\mathbb{Z})$ contient un seul élément $x \neq 0$; soit \tilde{G} l'extension correspondante de G par $\mathbb{Z}/2\mathbb{Z}$. Il résulte de (6.5.3) que L a une BNA si et seulement si l'homomorphisme $\varphi_L : \text{Gal}(k/k) \rightarrow G$ 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 $\text{SL}_2(\mathbf{F}_8)$ 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 $H^3(G, \mathbb{Z}/2\mathbb{Z})$ contient un seul élément $x \neq 0$, et l'on voit que L a une BNA si et seulement si $x_L = 0$ dans $H^3(k, \mathbb{Z}/2\mathbb{Z})$.

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 $q = (q_i)$ 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, q) par le G -torseur correspondant à L . On obtient ainsi une k -*forme* $(V, q)_L$ de (V, q) . On peut démontrer :

(6.6) - *Si L a une BNA, $(V, q)_L$ est isomorphe à (V, 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 $\varphi : \text{Gal}(k/k) \rightarrow G$, on a

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

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 $H^1(G, \mathbb{Z}/2\mathbb{Z})$, le cup-produit $ab(a+b)$ est un élément négligeable de $H^3(G, \mathbb{Z}/2\mathbb{Z})$.

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 $k = \mathbb{R}$.

(7.2) - *Supposons G abélien élémentaire d'ordre 2'. Si $x \in H^n(G, \mathbb{Z}/2\mathbb{Z})$, 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 $H^*(G, \mathbb{Z}/2\mathbb{Z})$ engendré par les $ab(a+b)$, où a et b parcourrent $H^1(G, \mathbb{Z}/2\mathbb{Z})$.

Il y a des résultats analogues pour $A = \mathbb{Z}/p\mathbb{Z}$, 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 étalés de la droite affine en caractéristique p* (*C.R. Acad. Sci. Paris*, 311, 1990, série I, 341-346).
 — *Spécialisation des éléments de $Br_2(Q(T_1, \dots, T_n))$* (*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

page	
1	Définitions
2	Historique
5	Références
9	Rappels sur la torsion
11	Octonions
13	Produits croisés
15	Rappels sur les formes quadratiques
20	Coniques et quaternions
23	La formule $\delta z = z^2$
25	Classes de cohomologie négligeables
26	Une formule de cobord
31	$B_{p,p} K$ en caract. $p > 0$
34	Invariants cohomologiques des formes quadratiques
36	Un autre invariant (rang pair ≥ 4 , disc. = 1)
41	$K^*/ND^* \rightarrow H^3(K)$ d'après Mercuri-Suslin
44	Anneau de Witt et conjectures de Milnor
50	Cohomologie du groupe orthogonal ; le groupe $\tilde{O}(q)$
53	(B. Kahn) Formes de Pfister
58	" Théorème d'Arason-Pfister
59	" Invariant d'Arason
61	" Existence de e_F^3, e_F^4 .
63	Retour à $O(q)$ et $\tilde{O}(q)$; les cobords δ^1 et δ^2
65	La formule $w_2(q_\alpha) = w_2(q) + w_1(q) \cdot \delta^1(\alpha) + \delta^2(\alpha)$
68	Remarque sur $H^1(K, G_2)$
68	Remarques sur la caract. 2
70	L'invariant i_3 à valeurs dans $H^3(K)$
72	Applications de i_3 à la cohomologie de G_2, F_4, E_8
77	Le cas de G_2
84	Le cas de F_4

88 Formes quadratiques : théorèmes d'injectivité du H^1
91 Théorème de Simplification d'Araujo-Pfister ($q \mapsto q \otimes q'$, $\text{rg } q'$ impa
92 ————— de Witt
94 ————— de Springer
100 Questions
101 Forme trace : cas des algèbres centrales simples ; p. 102 : alg. de rang 1
111 Retour à G_2 : table
112 Produit tensoriel de 2 algèbres de quaternions
114 Puissances divisées (si -1 est un carré)
118 Forme trace des corps et des algèbres étendues
120 q_E contient $\langle 1, \dots, 1 \rangle$, resp. $\langle 2, 1, \dots, 1 \rangle$
123 $H^1(S_n)$ et $H^2(S_n)$
126 La formule $w_2(q_E) = \varphi_E^*(s_n) + (2)w_1(q_E)$
131 Applications et exemples ; équation du 5^e degré
140 Le cas de A_6 ; l'invariant dans $H^3(K)$?
142 Automorphisme extérieur de A_6 ; 1. formule $q'_E \simeq 2q_E$
145 Retour S_n l'équation du 5^e degré (corps finis)
146 Algèbres à involution
149 Lien avec les groupes classiques
150 les deux théorèmes d'Albert
158 Corrections
158 Unitaires et hermitiens
160 $H^1(K, U_A) \simeq$ classes d'hermitiens inversibles
163 Invariants de teneurs quadratiques
165 Le théorème de Bayer-Busstra
168 (E. Bayer) Le théorème de simplification de Witt dans le cas hermitien
176 G-formes quadratiques
177 G-algèbres galoisiennes
179 BNA = belle base
181 Obstruction dans $H^1(K, U_G)$

181 Théorème de Bayen-Lousta
184 Le cas où $cd_2 K \leq 1$
188 Parenthèse sur la structure de U_G
191 Le cas où K est un corps des nombres et où $H^1(G) = H^2(G) = 0$
196 Le cas où le 2-Sylow de G est abélien élémentaire : énoncé
des résultats
200 Exemples
206 Démonstrations

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 $Q(T)$

Rappel de définitions

K corps, \overline{K} clôture algébrique

$|$
 K_s clôture séparable

$|$
 K

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

1^{er} contexte

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

G_K - module.

On définit $H^i(G_K, A) = \varinjlim_U H^i(G_K/N, A^U)$

U sg ouvert normal de G_K

H^i : facteurs dérivés du foncteur "points fixes"
 sur le complexe des cochaînes

$$f(g_1, \dots, g_i)$$

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

2^{ème} situation

A groupe commutatif où opère G_K

$$H^0(G_K, A) = A^G \quad (\text{invariants}) \quad \text{groupe}$$

$$H^1(G_K, A) = \lim_{\rightarrow} H^1(G_K/U, A^U)$$

G groupe qui opère sur A

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

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

$$= a_s a_t$$

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

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

c'est un ensemble pointé.

Petit historique

Brauer ~ 1929 dans 2 contextes

différents :	alg. centrales simples (groupe de Brauer)
	$H^2(G_K, K_s^*) = \text{Br}(K)$

via représentations linéaires de groupes (3)

Soit Γ un groupe fini

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

repr. irréduc. / \mathbb{C} de Γ
caractère à valeurs dans K

Peut-on la réaliser sur K ?

Sinon, pourquoi ?

Par isom. aux s^p , $s \in G_K$

$$s^p = \bar{A}_s \circ A_s$$

Est-ce que

$$A_{st} = A_s \circ A_t ?$$

Si oui, on peut remplacer \circ par
 \circ' tel que $s^p = p'$.

Ce n'est pas tout à fait vrai, mais
on a $c_{st} A_{st} = A_s \circ A_t \quad c_{st} \in K_s^*$

c_{st} est un 2-cocycle.

Sa classe dans H^2 est obstruction
au problème.

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

Tochtermüller ~ 1940

$\begin{smallmatrix} \subset & G \\ K & \end{smallmatrix}$

extension galoisienne finie

$\text{Br}(K) \hookrightarrow \text{Br}(\subset)^G$ surjectif

(4)

L'obstruction est un 3-cocycle : plus précisément un élément de $H^3(G, L^*)$ à image 0 dans $H^3(G_K, \mathbb{G}_m)$. descente et torsion : variantes 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 ~~descente~~ 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

Chernov 1989

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

Kneser, Harder

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

Références

LN 5

cohomologie non abélienne:

M. Kneser, Tata Institute

(Jacobson : coh. gal. dégénérée)

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. M. Lai, Etale cohomology (1980)

J. M. Lai, Duality theorems (~ 1986)

H. Koch

Platonov, Principe de Hasse
(à paraître).

Etude de $H^*(K, \text{groupe semi-simple})$

K quelconque ??

Cas orthogonal:

progrès grâce à Pfister, Markov - Sulim, Arason, Rost, Jacob, ...

Groupes exceptionnels ?

Qu'est-ce que: $G_1 \rightarrow G_2$

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

Exemple: $G_2 \hookrightarrow SO_+$

$$O(n) \rightarrow O(3n)$$

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

Injectif (Pfister)

Démonstration par systèmes de racines ??

$$K' \\ | \text{ fine}$$

$$K$$

est-ce que

c'est injectif ?

$$H^1(K, G) \rightarrow H^1(K', G)$$

"

$$H^1(K, R_K^{K'} G)$$

Springer: $[K':K]$ impair, cas orthogonal
 $\sim 1950 \Rightarrow$ injectif

B-Lauscha: Même énoncé pour groupes unitaires

$$E_6, E_7, E_8$$

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

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

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

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 T^n)

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

H^1 a comme base x_1, \dots, x_n
 $x_1 \wedge x_2, \dots$

$\dim \wedge$

$\dim (\wedge)$

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

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

\hookrightarrow 3-formes de Pfister

\hookrightarrow éléments décomposab(e)s.

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

$H^1(K, G_2) =$ él' neutre
s'espaces de dim 3
d'un espace vect / \mathbb{F}_2
de dim n.

pts rationnels / \mathbb{F}_2 de la Grassmannne
des 2-plans (projectifs) dans \mathbb{P}^{n-1} .

LN 5: ces H^1 sont finis.

$H^1(K, F_4)$: connu? T; fs.

Rappels :

L galinaire
 $| G$

K "objets" \times sur K

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

x_0 fixe

x tel que $x_L \cong x_{0L}$

classes de tels $x \longleftrightarrow H^1(G, \text{Aut}_L x_0)$

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 $a_s \in \text{Aut}_L x_0$

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

$$a_s \text{ est un cocycle: } a_{st} = \varphi^{-1} \circ s \varphi = \\ = \varphi^{-1} \circ (\varphi \circ a_t) = a_s \circ a_t.$$

φ modifié par un automorphisme de x_0
remplace a_s par un cocycle cohomologique

Injectivité: facile

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

descente de Weil.

classes d'objets sur K qui sont K_s -isom.

$$\tilde{\alpha} : X_0 = H^1(K, \text{Aut } X_0).$$

Exemples :

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

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

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

classes de formes quadratiques / K
non dégénérées de rang n

"

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

caract 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 caract 2 (n impair)

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

pas lisse en caract. 2 (1 pt avec n. chotents)

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

$$1 \rightarrow \mu_2 \rightarrow G_n \rightarrow G_n \rightarrow 1$$

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

O_n n impair

$\det : O_n \rightarrow \mu_2$, $SO_n = \ker(\det)$
 SO_n est lisse.

classes d'octonions ($= \text{ord. de Cayley}$)
 $(\text{car} \neq 2)$



$$e_0 = 1$$

Oct. base e_0, e_1, \dots, e_7

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

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

Mêmes règles pour tous les triangles.

"quaternions" sur e_i, e_{i+1}, e_{i+3}
 $i \bmod 7$.

Tous les octonions : $e_1^2 = \alpha, e_2^2 = \beta, e_3^2 = \gamma$
 $\alpha, \beta, \gamma \neq 0$.

$$e_4 = e_1 e_2, \quad e_4^2 = e_1 e_2 e_1 e_2 = -e_1 e_1 e_2 e_2 = -d \beta, \text{ etc.}$$

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 $\leftrightarrow H^1(K, \mathrm{Aut} M_n)$

$$H^1(K, \mathrm{PGL}_n)$$

$\mathrm{Br}(K; n)$: sous de $\mathrm{Br}(K)$ défini
par les alg. de rang " n^2 "

$$\mathrm{Br}(K; n) \simeq H^1(K, \mathrm{PGL}_n)$$

$$\mathrm{Br}(K) \cong \varinjlim_n H^1(K, \mathrm{PGL}_n)$$

(rel. div.)

Descente générale de Grothendieck
Topologie étale

Base : "1 point" $\mathrm{Spec} K$.

$$H^1(K, \mathbb{PGL}_n)$$

$$1 \rightarrow \mathbb{G}_m \rightarrow \mathbb{G}_{\text{a}} \rightarrow \mathbb{PGL}_n \rightarrow 1$$

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

α_s : 1-cocycle \mathbb{PGL}_n

b_s : relèvement dans \mathbb{G}_{a}

$$c_{st} = b_s^{-1} b_t b_{st}^{-1} \rightarrow 1 \text{ dans } \mathbb{PGL}_n$$

$$\begin{array}{ccc} 2\text{-cocycle} & \text{classe de } c_{st} = \Delta(\alpha) \\ & \alpha \text{ classe de } \alpha. \end{array}$$

On obtient ainsi

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

Thm C'est un isomorphisme.

Produit croisé

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

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

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

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

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

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

Algèbre centrale simple, assoc. γ

On le vérifie pour $\gamma = 1$ (alg. de matrices)
 cocycle se tue après ext. à \mathbb{C}
 \rightarrow vrai en général.

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

id. usuelle

(produits croisés)

On a un précédent

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

CG : les deux identifications diffèrent
 CL ! par un signe.

3^{ème} définition : Milne

Giraud

Grothendieck utilise l'identification par Δ .

1^{er} chapitre : Rappels sur les formes quadratiques

$\text{car}(K) \neq 2$.

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

Notation $= H^i(K)$.

H^i : suite exacte de Kummer

$$1 \rightarrow \mu_n \rightarrow \mathbb{G}_n \rightarrow \mathbb{G}_n \rightarrow 1 \quad \text{car } K \nmid n$$

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

$$K^* \xrightarrow{\quad} K^* \rightarrow H^i(K, \mu_n) \rightarrow 0$$

$$H^i(K, \mu_n) \cong K^*/K^{*^n} \quad \text{"fl. de Kummer"}$$

$n=2$: $H^i(K) = K^*/K^{*^2}$

$$(\alpha) \longleftrightarrow \alpha \in K^*$$

Notation additive

$$(\alpha b) = (\alpha) + (b)$$

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

$$0 \rightarrow H^2(K, \mu_n) \rightarrow \text{Br}(K) \xrightarrow{\quad} \text{Br}(K)$$

Alors $H^2(K, \mu_n) \cong \text{Br}_n(K)$ si $\text{car. } K \neq n$.

On choisit l'identificat. "produit croisé". (16)

$$H^2(K, \mathbb{Z}/_2\mathbb{Z}) \cong \text{Br}_2(K).$$

Cup-produit :

$$H_A^i \times H_B^j \longrightarrow H_c^{i+j} \quad \text{si } A \otimes B \rightarrow c.$$

au niveau des cocycles, facile à écrire

$f \quad g$

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

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

Cup-produit $H^1 \times H^1 \rightarrow H^2 \pmod{2}$:

$$K^*/K^{*2} \times K^*/K^{*2} \rightarrow \text{Br}_2(K)$$

Calcul montre que

$$a \in K^*, b \in K^* \rightarrow (a) \cup (b) = \begin{array}{l} \text{classe de} \\ \text{l'alg. quat} \\ (a)(b) \\ (a, b) \end{array}$$

$$i^2 = a, j^2 = b$$

Calcul. Plus intéressant de le faire pour n quelconque:

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

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

$$\underbrace{K^*/K^{*2}}_{b} \times \text{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})$$

(17)

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

construire algèbre centrale simple

$$(b) \cdot (x) \in \text{Br}_n(K).$$

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

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

$$H^2(G_{L/K}, L^*) = K^*/NL^* ; \text{ où } [b] \in H^2(G_{\bar{K}/K}, \bar{K}^*)$$

\uparrow
 b

$$\text{On a: } (b) \cdot (x) = -\text{cl}([b])$$

Signe -

Correction à l'historique :

- Il faut parler de Kneser et Harder pour la nullité de $H^1(K)$ totale imag si connexe ($\neq E_8$)
- Cas des variétés abéliennes (et c. e.p.)
- $\begin{array}{l} \rho = A_s \rho A_s^{-1} \\ c_{s,t} A_{st} = A_s^{-1} A_t \end{array} \} \text{ ne marche pas}$
- $\begin{array}{l} \rho = A_s^{-1} \rho A_s \text{ oui !} \end{array}$

Autres corrections

L/K cyclique d'ordre n

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

$$b \in K^* \quad [b] \in H^2(L/K, L^*) \hookrightarrow \text{Br}_n(K) = H^2(K, \mathbb{Z}/n\mathbb{Z})$$

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

$$[b]_x = \begin{cases} \pm(b) \cdot x \\ \alpha \end{cases} \text{ ds } H^2(K, \mu_n)$$

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

Signe correct : —

Preuve :

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

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

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

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

$$b \cdot \delta_x = \delta_x \cdot b \in H^2(K, \mathbb{G}_m) = \text{Br}(K)$$

$$d^0 \mathbb{Z} \quad 0. \quad (\text{les 2 classes commutent})$$

On a :

$$[b]_x = \delta_x \circ b$$

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

On se donne

$$\begin{aligned} \chi &\in H^1(G, \mathbb{Z}/m\mathbb{Z}) = \text{Hom}(G, \mathbb{Z}/m\mathbb{Z}) \\ m &\in H^0(G, M) \end{aligned}$$

$$\begin{aligned} \delta \chi \cdot m &\in H^2(G, M) & \delta \chi &\in H^2(G, \mathbb{Z}) & \delta m &\in H^1(G, M_n) \\ \chi \cdot \delta m &= -\delta m \cdot \chi & &\in H^2(G, M_n) \\ i(\chi \cdot \delta m) &\in H^2(G, M) \end{aligned}$$

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

$$\stackrel{11}{(-i(\delta m \cdot \chi))}$$

Le résultat souhaité s'en déduit

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

$\delta \chi$ est représenté par le cocycle

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

δm On choisit $x \in M$ avec $mx = m$

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

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

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

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

(Δ x à valeurs dans $\mathbb{Z}/m\mathbb{Z}$, pour distribuer la parenthèse, il faut utiliser F).

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

(Ou encore: règle de leibniz!)

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

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

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

$$(a)(b) \in H^2(K) = \text{Br}_2(K)$$

$(a)(b)$ représenté par l'alg. de quaternions
 $(a, b) \quad i^2 = a, \quad j^2 = b, \quad ij = -ji$

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

On peut lui associer $\text{inv}(C) \in \text{Br}_2(K) \supset H^1(K, \text{PG}_2)$

C devient isomorphe à P , sur $K_S \quad \text{Br}''(K, 2)$

C décrit par un élément de $H^1(K, \text{PG}_2)$

Conique associée à $(a, b) \quad ax^2 + by^2 - abz^2 = 0$.

D alg. de quaternions (a, b)

$$\begin{cases} \text{Trd} = 0 \\ \text{Nrd} = 0. \end{cases} \quad \begin{cases} x_i + y_j + z_{ij} = 0, \\ -ax^2 - b y^2 + ab z^2 = 0. \end{cases}$$

Autre interprétation

équat minimale $x^2 - \text{Trd}(x)x + \text{Nrd}(x) = 0$.

CCD): cône des élts de D de \square nul.

F: alg. de quaternions $\xrightarrow{\text{isom.}} \text{conique}$
 $\xrightarrow{C_2}$

ι_K commute aux ext. de scolaires

et 1-cocycle ds Aut \mathcal{D} , $\mathcal{D} \in \mathcal{C}$,

$$F(\iota_K \mathcal{D}) = \iota_K F(\mathcal{D}) \quad (\text{cf LN 5}).$$

Δ for torsion à partir de $\mathcal{D} = M_2$

$$F(\Delta) = \iota_K F(\mathcal{D}) \quad F(\mathcal{D}) = P_1$$

car $x \in M_2$ $x \neq 0$.

$$\text{Im } x = L \text{ droite} \quad (\hookrightarrow P_1)$$

, d'où $F(\Delta)$ est un P_1 tordu

Soit C de genre 0, construire \mathcal{D} à partir de C ?

Intrinsèquement (pour chx coord, cf + ht)

On fabrique un fibré E vectoriel de rang 2 sur C

$$\mathcal{D} = \text{End}_K(E).$$

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

Si P_1 , E décomposable.

Construction de E :

$C \times C$ Δ diagonale $\mathcal{O}_{C \times C}(\Delta)$ fibré de rang 1

$$\downarrow \pi = \pi_1 \circ \pi_2$$

$$E = \pi_* \mathcal{O}_{C \times C}(\Delta)$$

$$(\text{et } \pi_* \mathcal{O} = \mathcal{O})$$

(fctions aux pt + un pôle simple sur Δ).

La fibre en P , $E_P =$ fctions rotationnelles sur C aux pt plus 1 pôle simple en P , est de dimension 2.

$$0 \rightarrow \frac{1}{(\text{fibré trivial})} \rightarrow E \rightarrow T \rightarrow 0.$$

fibré tgl

$$H^1(C, \text{Hom}(\mathbb{T}, 1)) = H^1(C, \mathbb{G})$$

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

(Prob' ± 1, car sinon on a une des erreurs dans la correspondance à ce niveau, ce qui n'est pas).

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

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

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

Formules évidentes

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

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

$(a)(b) = 0$ si l'éq $ax^2 + by^2 - abz^2 = 0$ a une solution $\neq (0, 0, 0)$ ds $K \Leftrightarrow b$ norme de l'ext. $K(\sqrt{a})/K \Leftrightarrow$ norme ds $K(\sqrt{b})/K$.

$$1^{\text{e}} \text{ cas} \quad ax^2 - ay^2 + a^2z^2 = 0 \quad x=1, y=1, z=0.$$

$$2^{\text{e}} \text{ cas} \quad ax^2 + (1-a)y^2 - a(1-a)z^2 = 0$$

$$\text{ou encore } z^2 - ax^2 - (1-a)y^2 = 0. \quad x=y=z=$$

Débouche sur la K -théorie de Milnor . . .

On va détailler un peu $(a)(\alpha) = (-1)(\alpha)$. (23)

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

$$\delta: H^i(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^{i+1}(G, \mathbb{Z}/2\mathbb{Z}).$$

$$\delta x = 0.$$

Formule $\boxed{\delta x = x^2}$ si $i=1$

Opération de Bockstein (modulo p)
 $= Sq^1$ (pui. de Steen)

Pour démontrer cela, on utilise exemple universel
 $x \in H^i(X, A)$

X complete simpl. par ex.
 i, A fixé

On veut trouver une formule pour $\delta x, x \dots$

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

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

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

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

Ici $S_N / \mathbb{Z} = P_N(\mathbb{R})$ S_N : sphère
 $\pi_i = \mathbb{Z}/2\mathbb{Z}$

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

" $N = \infty$ " 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 polynômes en $i \in \mathbb{H}^1$

$$1, z, z^2, z^3, \dots$$

$$\delta_L = \begin{cases} 0 & \text{mais si } 0, \text{ vrai toujours (impos.)} \\ z^2 & \text{Donc c'est } z^2. \end{cases}$$

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

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

G_2 gr. cycl. d'ordre 2

$$G_1 \xrightarrow{f} G_2$$

$$xe = f^*(e)$$

En fait, même preuve car $BG_2 = K(\mathbb{Z}/2\mathbb{Z}, 1)$

" classifiant
de G_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 $i \in K$, $\neq 0$ si i non

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

Cor: Si car $K = \mathbb{F}_p$ $\quad p \equiv 1 \pmod{4} \Rightarrow (-1) = 0$

$$\delta x = 0$$

classes de cohomologie "négligeables"

G fini, M G -module

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

Déf.: x négligeable (si f finie) si pour tout homomorphisme: $G_K \xrightarrow{f} G$,
 $f^* x = 0$ dans $H^i(K, M)$.

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

En fait, il y a beaucoup de telles classes
 $H^i_{\text{while}}(G, M) = H^i / H^i_{\text{négl}}$ "petit".

Exemples: 1. 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 $G = (2, \dots, 2)$

$H^*(G)$ = alg. de polyg 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 de $H^1(K), H^1(K), H^3(K)$.

car $K = 2 \Rightarrow H^i(K) = 0$ à partir de 2

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

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

Quelques remarques "négligeables"

- Dans le cas des 2-gps, les classes nég. st l'idéal engendré par $(v^2 u + u v^2)$
- Si K car p , $\mathbb{F} \equiv 1 \pmod{4}$
(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
 $\delta: H^1 \rightarrow H^2$

On utilise Mercuriev-Suslin : Tout él. 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 $u, v \in H^1(G_K)$.

$$\delta(u, v) = \delta u \cdot v + u \cdot \delta v = u^2 v + u v^2$$

Une formule de cobord.

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

suite exacte de G -modules

Soit χ_s 1-cocycle de G à valeurs ds $\text{Hom}(C, A)$. 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 $\delta: H^i(G, C) \rightarrow H^{i+1}(G, A)$
et

$\delta_\chi : H^i(G, C) \rightarrow H^{i+1}(G, A)$ les cobords correspondants. (27)

Formule: $\delta_\chi(x) = \delta(x) + (\chi) \cdot x$

$x \in H^i(G, C) \quad (\chi) \in H^i(G, \text{Hom}(C, A))$

$C \times \text{Hom}(C, A) \rightarrow A$.

Preuve: $f = f(s_1, \dots, s_i)$ i-cochaîne de \mathcal{B} relevant un cocycle de C, f , de classe x

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

$f(s_1, s_2, \dots, \dots) +$

$\delta_\chi \mapsto \overset{s_1}{f}(\quad) - \dots$

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

$s_1, \dots, s_{i+1} \mapsto \chi_s (\overset{s_1}{f}_c(s_2, \dots, s_{i+1}))$

"cup-product"

Applications (car $K+2$)

* $\delta \circ c = (-1) \circ c$

$0 \rightarrow \mathbb{Z}_2 \rightarrow \mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \rightarrow 0 \quad (*)$.

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

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

$\chi = (-1)$

$$\delta_{(*)} : H^1(K, \mu_p) \rightarrow H^2(K, \mu_{p^2})$$

$\delta_{(*)}$ associé à $(*)$ est 0

$$H^1(K, \mu_m) = K^* / K^{*^m}$$

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

surjective !

$$0 = \delta_{*}(x) = \delta(x) + (x)(-1) \rightarrow \delta(x) = (x)(-1).$$

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

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

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

$$\text{Bockstein} \quad 0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z} \rightarrow 0$$

$$\delta x ? \quad x \in H^i(K)$$

$$\varphi \in H^i(K) \text{ associé à } \mu_{p^2}$$

$$\text{L'action de } G_K \text{ sur } \mu_{p^2} \text{ définit } \varphi: G_K \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^* \subseteq \mathbb{Z}/p^2\mathbb{Z}$$

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

$$\Leftrightarrow \text{m classe mod } p^2 \quad (m, p) = 1.$$

$$\frac{m^{p-1} - 1}{p} = -\varepsilon(m) \pmod{p}.$$

$$\boxed{\delta x = x \cdot \varphi} \quad x \in H^i(K)$$

$$\varphi \in H^i(K)$$

2 preuves : Il suffit de prouver cette formule

quand K contient μ_p (car $\kappa' = k(\mu_p)$ K de d^0 1^{er} sp + 29)
et donc $H^i(K, \mathbb{Z}) \hookrightarrow H^i(K')$.

$$\varphi: G_K \rightarrow \mathbb{Z}/p\mathbb{Z} = \{ \text{elts} \equiv 1 \pmod{p} \pmod{p^2} \}$$

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

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

$$0 \rightarrow \mu_p \rightarrow \mu_{p^2} \rightarrow \mu_p \rightarrow 0$$

$$\left\{ \begin{array}{l} \mu_p = \mathbb{Z}/p\mathbb{Z} \text{ via } z \\ \psi \text{ tord l'action de } \mu_p \\ z^p = z \end{array} \right. \quad \text{si } \varphi: \delta z = z^{1+\varepsilon(\delta)} = z \cdot z$$

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

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

Corollaire G fini $p \neq 2$

$$u \in H^1(G)$$

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

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

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

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

$$G = C_p \quad \dim_{\mathbb{Z}/p\mathbb{Z}} H^i(G) = 1 \text{ pour tout } i, \text{ négligeable pour } i \geq 2$$

$$\begin{array}{cccc} H^0 & 1 & H^2 & \delta u \\ H^1 & u & H^3 & u \cdot \delta u \\ & & H^4 & \delta u \cdot \delta u \end{array}$$

Compléments1) Coh. "négligeable"

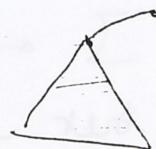
$$\begin{array}{c} x \in H^i(G, V) \\ K \quad G_K \xrightarrow{\varphi} G \\ \text{Gal}(K/\mathbb{K}) \end{array} \quad \begin{array}{l} G \text{ fini} \\ \varphi^* x = 0 \end{array}$$

$$\begin{array}{ccc} Y & & \\ \downarrow & G & H^*(G) \rightarrow H^*(X) \\ X & \rightarrow BG \\ \text{Analogue} \end{array}$$

Cohom. négligeable pour la top. étole $\Leftrightarrow x = 0$
top. usuelle

 BG classifiant
du gpe G so cohom est celle de G .d'où le résultat pour la top. usuelle.Pour "étole" X complexe simplicial fini
 $\begin{cases} \text{esp. alg. / } \mathbb{C} \text{ qui a le même} \\ \text{(affine)} \end{cases}$

type d'homotopie
que X .



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

$\text{supp}(x_i) \subset \text{complexe}$

On fabrique l'espace en supprimant les cond. réelles
soit $z_i, z_i \in \mathbb{C}, \sum z_i = 1$, support $\subset \text{comp}$.

$$\begin{array}{c} \text{Ex} \quad X \xrightarrow{\quad} x_1, x_2 \quad x_1 + x_2 = 1 \\ \quad \quad \quad n_i \geq 0 \end{array}$$

X_0 / plan complexe à m 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)
ou var de Stiefel.

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

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

$V_{N,n}$ GL_n opère libre sur $V_{N,n}$

$$G \subset GL_n$$

G opère librement sur $V_{N,n}$

$V_{N,n}$ var. lisse connexe, à cohom. nulle



$$V_{N,n}/G$$

jusqu'à $2N - (2n+1)$ (?)
 $\rightarrow \infty$ avec N .

$H^*(G) \rightarrow H^*(V_{N,n}/G)$ injectif jusqu'à cette dim.
 N grand: pas de classes négligeables!

Mais: Y

$$\downarrow G$$

X négligeable

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

2) K car. $p > 0$.

Décrire $\text{Br}_p K$?

Produits croisés cycliques

10) $a \in K$, $b \in K^*$ donnés
 $[a, b] \in \text{Br}_p K$

a définit une extension de type Artin-Schreier $x^p - x = 0$
et $y^p = b$ $yy^{-1} = x + 1$.

$$\begin{matrix} K_a \\ | \\ \mathbb{Z}/p\mathbb{Z} \\ \times \end{matrix}$$

$[a, b] = 0 \iff b$ est une norme de K_a
 $\xi \in \text{Br}_p K$ est de la forme $[a, b]$
 a imposé $\iff \xi$ scinde (= annulé par K_a)

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

② $a, b \in K$

(32)

$[a, b] \in \text{Br}_p K$

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

$[a, b] = [ab, b] \quad \text{si } b \neq 0$
 $= 0 \quad \text{si } b = 0.$

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

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

$d(bc) = bdc + cbd$

$\Omega^1 K \rightarrow \text{Br}_p K$

$\sum a_i db_i \mapsto \sum [a_i, b_i] \in \text{Br}_p K$

$\sum a_i \frac{db_i}{b_i} \mapsto \sum [a_i, b_i] \in \text{Br}_p K$

Albert, Witt, ...

C'est sayechf, les diff. exactes db donnent 0 ds Br_p

$\Omega^1 K \xrightarrow{F^{-1}} \Omega^1 K / dK \rightarrow \text{Br}_p K \rightarrow 0.$

$F: \sum a_i \frac{db_i}{b_i} \mapsto \sum a_i^p \frac{db_i}{b_i} \in \Omega^1 K / dK$

= "inverse de l'opérateur de Cartier"

cf Witt Hamb. Abhandl. 1958

Pour $p = 2$

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

$$x^2 + a'y^2 + b'z^2 + yz = 0.$$

$[a, b] \mapsto x^2 + b'y^2 + abz^2 + byz = 0$

3°)

C genre 0.

$0 \rightarrow 1 \rightarrow E \rightarrow T \rightarrow 0$.

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

La construction est tout à fait universelle

$x = m \in \mathbb{Z}$ $P, 1 \in \mathbb{Z}$.

p premier $\Rightarrow p+m$

car sinon en car p , l'extension serait triviale
donc $m = \pm 1$

Formes quadratiques et leurs invariants cohomologiques

car $K \neq \mathbb{Q}$.

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

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

• langage sur V de dim finie, muni d'une forme quad. (non dég.) (à isom. près)

• langage $f(x_1, \dots, x_n) = \sum a_{ij} x_i x_j \quad a_{ij} = a_{ji} \quad a_{ij} \in K$
 $f \sim f'$ s'il existe une transf. universelle des x_i amenant f sur f' .
 $(a'_{ij}) = {}^t C \cdot (a_{ij}) C$. avec $C \in GL_n$.

$$f \sim \sum a_i x_i^2 \quad a_i \in K^* \quad \begin{cases} x \cdot x = q(x) \\ x \cdot y = \frac{1}{2}(q(x+y) - q(x) - q(y)) \end{cases}$$

V a une base orthogonale (e_i) $e_i \cdot e_j = 0 \quad i \neq j$.

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

$$\langle a_1, \dots, a_n \rangle \stackrel{?}{=} \langle b_1, \dots, b_n \rangle$$

Les formes à deux variables décident de cette question

$n \geq 2$ $\{a_{11}, \dots, a_{nn}\}, \{b_{11}, \dots, b_{nn}\}$ sont 2-voisines si
 $a_{ii} = b_{ii}$ pour tout i sauf au plus 2 valeurs.
et $\langle a_{ij}, a_{ik} \rangle = \langle b_{ij}, b_{ik} \rangle$.

Thm (Witt) Si $\langle a_{11}, \dots, a_{nn} \rangle \simeq \langle b_{11}, \dots, b_{nn} \rangle$, il existe une chaîne (finie) de formes 2-voisines de la précédente offrant $\langle a_{11}, \dots, a_{nn} \rangle \simeq \langle b_{11}, \dots, b_{nn} \rangle$.

ie le graphe des $\langle b_{11}, \dots, b_{nn} \rangle \simeq \langle a_{11}, \dots, a_{nn} \rangle$ est connexe (arête existe si formes 2-voisines)

$V, q \quad m \geq 3$

(35)

$\mathcal{E} = (e_1, \dots, e_n)$ 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 connex

" Générateurs : formes à 1 variables

Relations : formes à 2 variables "

Ce principe va permettre de définir des invariants

Inv. cohé m: classes de Stiefel-Whitney
(cf Delzant, fin des années 50).

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

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

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

$i \geq 0$.

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

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

$\alpha \in K^* \mapsto (\alpha) \in H^*(K) = K^* / K^{*2}$ fait additiveme

$$w_1(q) = \sum (\alpha_i) = (\alpha_1, -\alpha_n) = (d)$$

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

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

Prop (Delzant) Si $\langle \alpha_1, \dots, \alpha_n \rangle \cong \langle \beta_1, \dots, \beta_n \rangle$, alors

$$\prod (1 + (\alpha_i)) = \prod (1 + (\beta_i)) \text{ dans } H(K)$$

On est ramené au cas $m=2$

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

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

\sqrt{q} e.v. quad.

alg. de Clifford $C(V)$

$$\text{eng. par } V \quad x \in V \quad x \cdot x = q(x)$$

$$C(V) = \text{alg. de quat. } (\alpha_1, \alpha_2) \quad e_1^2 = \alpha_1 \quad e_1 e_2 = -e_2^2$$

idem sur β d'où l'égalité.

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

$$w_m(q) = \pi(\alpha_i) \in H^m(K)$$

$w_2(q)$ = "invariant de Hasse-Witt".

$$w_2 = w_1 w_2 \quad \sum(\alpha_i) \sum_{j < k} (\alpha_j)(\alpha_k) = 3w_3 + \sum_{j < k} (\alpha_j)(\alpha_j)(\alpha_k) + (\alpha_j)(\alpha_k)(\alpha_k).$$

• $3 \bmod 2$, c'est 1 !

• le reste est négligeable

$$(\alpha_j)^2(\alpha_k) + (\alpha_j)(\alpha_k)^2$$

$$0 = (-1)(\alpha_j)(\alpha_k) + (\alpha_j)(-1)(\alpha_k)$$

cf Milnor (Invent. Math.) Si i n'est pas une puissance de 2, w_i peut s'écrire comme polynôme en les w_j , $j < 1$. Plus précisément :

Si l'on écrit $i = 2^{r_1} + 2^{r_2} + \dots + 2^{r_k}$, $r_1 < \dots < r_k$,

$$\text{on a : } w_i = w_{2^{r_1}} \dots w_{2^{r_k}}.$$

Autre invariant (n pair ≥ 4)

$$\textcircled{1} (d) = (1) = 0$$

$$q = \langle \alpha_1, \dots, \alpha_n \rangle \quad i(q) = (\alpha_1) \dots (\alpha_{n-1}) \in H^{n-1}(K)$$

Proposition: $\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle \beta_1, \dots, \beta_n \rangle$

$$\Rightarrow (\alpha_1) \dots (\alpha_{n-1}) = (\beta_1) \dots (\beta_{n-1}) \in H^{n-1}(K)$$

(37)

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

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

$$(\alpha_m) = (\alpha_1) + \cdots + (\alpha_{m-1})$$

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

$$= (\alpha_1)(\alpha_2) \cdots (\alpha_{n-1}) + \underbrace{(\alpha_2)(\alpha_3) \cdots (\alpha_{n-1})}_{\text{pour le } m-2 \text{ème terme}}$$

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

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

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

② Cas général

$$d \text{ disc. } (d) = w,$$

invariant $i(q) \in H^{m-1}(k)/w, H^{n-2}(k)$

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

$$K_d = K(\sqrt{d}) \quad d \text{ non carré}$$

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

$$K_d = K(\sqrt{d}) \quad \text{Prop: } H^i(K) \xrightarrow{\text{Res}} H^i(K_d) \xrightarrow{\text{Cor.}} H^i(K) \xrightarrow{x \mapsto dx}$$

Suite exacte

$$H^i(K)/dH^i(K) \hookrightarrow H^i(K_d)$$

38

Suite exacte des extensions quadratiques

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

Soit G un groupe profini et H un sousgroupe de noyau H . Soit $\varepsilon: G \rightarrow \{+1, -1\}$ le caractère

A G -module

soit module A "tordu par \mathbb{Z}_2 ". On a la suite exacte :

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

$\delta \circ c = a_\varepsilon \cdot x$

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

représenté par le cocycle $\tilde{\alpha}_2$ par

Rque $G \rightarrow G/\mathbb{H}$ $H^1(G/\mathbb{H}, \mathbb{Z}_\varepsilon) = \mathbb{Z}/2\mathbb{Z} \hookrightarrow H^1(G, \mathbb{Z})$
 si G purfini, c'est un isomorph

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

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

A^* : module indict $\text{Ind}_H^G A = A \otimes_{\mathbb{Z}} [G/H]$

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

$$0 \rightarrow \mathbb{Z}_2 \rightarrow \mathbb{Z}[G/H] \rightarrow \mathbb{Z} \rightarrow 0$$

$$e_1 - e_2 \quad e_1, e_2 \quad \rightarrow 1$$

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

mais l'action de groupe est une action forcée !

On a vu une formule générale la dernière fois pour les "tordues" \rightarrow avec produit, ici $\alpha_i \cdot x$.

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 cané et 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 $q_3 \sim q_3' \Rightarrow q \sim q'$
(cf prochaine fois)

On est ramené au cas :

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

et discrimin.

dq et dq' ont disc. 1.

On a des formules donnant $w_i(2q)$ en termes de (α, β) et de $w_i(q)$.

$$q = \langle \alpha, \beta, \gamma \rangle \quad \lambda \in K^* \quad \lambda q = \langle 2\alpha, 2\beta, 2\gamma \rangle$$

$$w_2(2q) = (\lambda\alpha)(\lambda\beta) + (\lambda\alpha)(\lambda\gamma) + (\lambda\beta)(\lambda\gamma)$$

$$= ((\alpha) + (\beta)) ((\alpha) + (\beta)) + \dots$$

$$w_2(2q) = (\lambda)(\lambda) + w_2(q)$$

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

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

La forme $q = \langle \alpha, \beta, -\alpha\beta \rangle$

$$-q \stackrel{\sim}{=} -\alpha x^2 - \beta y^2 + \beta z^2 = \text{Norme (alg. de quatr.)}$$

sur les elts de trace 0.

$$\begin{aligned}
 w_2(q) &= (\alpha)(\beta) + (\alpha)(\alpha\beta) + (\beta)(\alpha\beta) \\
 &\stackrel{(40)}{=} 3(\alpha)(\beta) + (\alpha)(\alpha) + (\beta)(\beta) + (-1)(\alpha) + (-1)(\beta) \\
 &= (\alpha)(\beta) + \cancel{(-1)(\alpha\beta)} \\
 w_2(q) &= (\alpha)(\beta)
 \end{aligned}$$

Remarque: On considère ici comme forme trinôme les sommes ob courrées, d'inv. nul.

Mais la forme naturelle en rg pair serait plutôt la forme hyperbolique. On verra les formules correspondantes la prochaine fois.

$$n=4 \quad q = \langle \alpha_1 \rangle \otimes (\langle 1 \rangle + \langle 2 \rangle + \langle \mu \rangle + \langle 2\mu \rangle)$$

Norme d'une alg. ob quaternions
(-2, -\mu)

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

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

w_2 déterminée

i — classe de α_1 modulo les normes rédui

$$K^*/IND^* \longrightarrow H^3(K)$$

$$x \in K^* \longmapsto (x) \cdot [D] \quad \text{cf prochaine fois.}$$

K car $\neq 2$.

$$q \quad w_1(q) \in H^i(K) = H^i(G_K, \mathbb{Z}/2\mathbb{Z}).$$

Range $q \leq 3$ w_1, w_2 classifiant

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

q

dis now \square ?

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

$$q = \langle a_1 \rangle \otimes (\langle 1 \rangle \oplus \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \langle b_1, b_2 \rangle) \quad \begin{matrix} a_2 = a \\ a_3 = q, b \end{matrix}$$

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

$$\begin{aligned} w_2(q) &= (b_1)(b_2) + (b_1)(b_1, b_2) + (b_2)(b_1, b_2) \\ &= (b_1)(b_2) + (-1, b_1, b_2) \\ &= (-b_1)(-b_2) + (-1)(-1) \end{aligned}$$

$$[D_q] \in H^2(K)$$

$$\text{``} \quad w_2(q) + (-1)(-1).$$

$$q \quad \left\{ \begin{array}{l} \text{alg. de quat} \\ \underline{a} \in K^* / N\mathbb{D}^* \end{array} \right.$$

Thème Mercurie Suslin

$$K^* / N\mathbb{D}^* \longrightarrow H^3(K)$$

$$a \in K^* \longmapsto \underline{(a)}: [D]$$

(on trouve 0 si a est une norme)

Cet homomorphisme est injectif

$$\begin{aligned} i(q) &= (a_1)(a_1, b_1)(a_1, b_2) = (a_1)(-1)(-1) + (a_1)(-1) \\ &\quad + (a_1)(-1)(b_2) + (a_1)(b_1)(b_2) \\ &= (a_1)[D_q]. \end{aligned}$$

C'est faux si le disc. n'est pas \mathbb{Z} .

$$i(q) \in H^3(K) / (d) H^0(K) \subset H^3(K_d)$$

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

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

$$w_2(\lambda q) = m_2(\lambda)(-i) + n_2(\lambda)w_1(q) + w_2(q)$$

$$m_1 = m-1 \quad m_2 = \frac{m(m-1)}{2} \equiv 0 \pmod{2}$$

$$n=4: \equiv 1 \pmod{2}$$

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

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 et où $dq \neq q$ sur $K = \mathbb{Q}(i)$ $\alpha, \beta \in K^*$ $(\alpha, \beta) \neq 0$.

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

~~•~~ = corps de quaternions ramif. en $2+i$ et 3 .

$$K = \mathbb{Q}(T) \quad T \text{ indép.}$$

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

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

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

Ou bien: classif. des formes

$$q \oplus (-dq) \quad 8 \text{ variables}$$

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 $q \oplus (-dq)$ est anisotrope.

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

lemme:

Sur k $q_1(x), q_2(x)$ anisotropes sur k alors $q_1 \oplus \bar{q}_2$ l'est sur $k(T)$.

Plus généralement d'ailleurs, K val. disc avec car 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

$$H^2(K) = 0 \quad (K \text{ fini})$$

W_1, W_2

$H^3(K) = 0$ (ex: corps de nbrs totalem imagin; corps de nbrs d'une var sur un corps fini)

W_1, W_2 , signatures aux places réelles

corps de nbrs.

(ou p. ch. de Shefel Whitney..)

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

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

$$w'(q) = w(q) / w(R)^m$$

$$= w(q) / [1 + (-1)]^m$$

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

$$w'(q) = 1 \text{ si } q \text{ hyperbolique}$$

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

$$w(R) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$H^0 \quad H^1$$

$$(1 + w'_1(q) + w'_2(q) + \dots) (1 + m(-1) + m_2(-1)(-1) + \dots) \\ = 1 + w'_1(q) + w'_2(q) + \dots \quad m_2 = \frac{m(m-1)}{2}$$

$$w'_1 + m(-1) = w_1$$

$$w'_2 + m(-1)w'_1 + m_2(-1)(-1) = w_2 \quad \dots$$

d'où $\omega = (-1)^{\frac{m^2}{4}} d$. $d \rightarrow m \equiv 0 \pmod{4}$
 $-d \rightarrow m \equiv 2 \pmod{4}$

Pour $m=2 \quad w'_2 = w_2 + (-1)(-1) + (-1)w_1$

$$q = \langle \alpha, \beta \rangle \quad w'_2 = (-\alpha)(-\beta) \quad \text{clifford de } (q)$$

$$m=4 \quad w'_1 = w_1 \\ w'_2 = [D_q]$$

$\mathbb{F} \in K$ corps de caract + 2

Anneau de Witt : \rightarrow Grothendieck-Witt
 notation (fâcheuse !) \widetilde{GrW}_α

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

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

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

produit = produit tensoriel.

Anneau de Witt $W = GrW/\alpha$ α engendré par

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

$$f_m \otimes h \simeq mh \quad \langle \alpha, -\alpha \rangle = \langle 1, -1 \rangle$$

$$"W = W_F" =: GrW/\alpha$$

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

rang mod 2

$I_F = \text{Ker } [W_F \rightarrow \mathbb{Z}/2\mathbb{Z}]$ classes des formes de rang 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) $K_m(F) = K_m^*(F) / 2 K_m^*(F)$

Qu'est-ce que $K_m^*(F)$? anneau gradué, engendré par des éléments de degré 1, relations de degré 2 ou 1.

$x \in F^* \mapsto \{x\} \in K_1^*(F)$ générat.

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

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

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

On dispose de flèches

$$K_m(F) \xrightarrow{\alpha} I_F^m / I_F^{m+1}$$

$$\beta \searrow \xrightarrow{\quad} H^m(F)$$

flèches faciles à définir, α sujective.

Conjecture: Ce sont des isomorphismes

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

$$k_F \xrightarrow{\alpha} I_F^n / I_F^{n+1}$$

$$\beta \downarrow \quad \downarrow e_F^n$$

$$e_F^n : I_F^n / I_F^{n+1} \xrightarrow{\sim} H^n(F)$$

$$\text{On note } e_F^n : I_F^n \rightarrow H^n(F)$$

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

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

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

$$\beta: \{x\} \mapsto (x) \in H^1(F)$$

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

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

$$\alpha: \{x\} \mapsto ? \in I_F^n / I_F^{n+2}$$

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

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

forme de ng 0.

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

les 2 formes sont égales mod I_F^{n+2} :

$$\langle x \rangle + \langle -x \rangle = 0 \text{ ds } W_F$$

$$\frac{1}{2} (\langle 1 \rangle - \langle x \rangle) \in I_F^{n+2}$$

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

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

$$m=1 \quad k_1 F = F^* / F^{*^2} \xrightarrow{\sim} I_F / I_F^2 \quad (47)$$

↓

trivial! $H^1(F)$

$$m=2 \quad k_2 F \xrightarrow{\sim} I_F^2 / I_F^3 \quad (\text{Milnor})$$

↓
Merkuriev
~1980. $H^2(F)$

$m=3$ α, β isomorphismes
Merkuriev - Suslin preprint 1986
Rost — 1986

$m=4$ e_F^4 existe Jacob - Rost Inv. Mat. 96 1989
Shierski Dokl. 308 1989

On peut aussi introduire $\frac{F_q}{F}$ plus grande 2-ext. def
(ie ext gal. à gpe de Galois un mu-2-gpe)

$\text{Gal}(F_q | F) =$ plus grand mu-2-quotient de G_F
:= $G_F(2)$

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

!!

$$H_q^m(F)$$

("cohomologie quadratique de F ")

$$\text{Si } \alpha: k_n \rightarrow I^m / I^{m+1}$$

$$\beta: k_n \rightarrow H^n$$

Si les β sont sujets (en dim $\leq n$) alors $H^m_q(F) \rightarrow H^m(F)$ est un isom.

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

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

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

$$k^m_F \rightarrow I_F^m / I_F^{m+1}$$

$$\begin{array}{c} \downarrow \\ H_q^m(F) \\ \downarrow \\ H^n(F) \end{array}$$

Conjectureusement, toutes les flèches sont des isomorphismes

q, q' formes de rang n

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

$$w_2(q) = w_2(q') \rightarrow \iota(q, q') \in H^3(K)$$

$$Q = q \oplus (-q') \quad \text{rang } 2n \text{ paire}$$

$$Q \rightarrow [Q] \in I_F^3$$

~~Lemma~~ $[Q] \in I_F^3$

~~$w'(Q) = \frac{1}{w'(q)} \quad \text{car } q \oplus -q \text{ hyp.}$~~

~~Soit $w'(q) w'(-q) = -1$.~~

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

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

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

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

Thme Si $m \leq 7$, $i(q, q')$ 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 $< 2^m$ et
 app $\bar{e} \in \mathbb{I}_F^{m+1}$, alors Q est hyperbolique.

$$Q = q \oplus -q \quad m = 4 \dots$$

cf Lam ou l'article original de Pfister

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

donc $Q \in \mathbb{I}^4$, donc hyperbolique, i.e. $q \sim q'$

Que i est un invariant relatif

$\Leftrightarrow q \text{ relatif du } \square$
 $q \text{ à Norme.}$

$$i(q) =: i(\text{Norme}, \text{Norme})$$

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.

$$\rightarrow SO(q) \xrightarrow{(\pm 1)} O(q) \xrightarrow{\{\pm 1\}} 1$$

Spin(q)

$$\downarrow \hookrightarrow O(q)$$

revêtu univers à 2 feuilles
simpl. connexe.

$$\begin{array}{c} \{ \pm 1 \} \\ \downarrow \\ \tilde{O}(q) \\ \hookrightarrow \\ O(q) \\ \downarrow \\ 1 \end{array}$$

On peut associer canonique à q un revêtu à 2 feuilles redonnant le gpe des spinneurs sur SO .

Si $q \rightarrow 2q$, $SO(q) = SO(2q)$, $Spin(q) = Spin(2q)$,
mais $\tilde{O}(2q) \neq \tilde{O}(q)$.

$C = C(q) = \text{alg. de Clifford de } q$

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

C eng. par V avec les relations \hookrightarrow

pour tout $x \in V$

$$\Rightarrow x \cdot y = -y \cdot x \quad \text{si } \theta(x) \text{ et } y \perp \text{ pour } q.$$

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

anti-autom $x \mapsto x'$ de C caractérisé par $x'x = 1$
si $x \in V$.

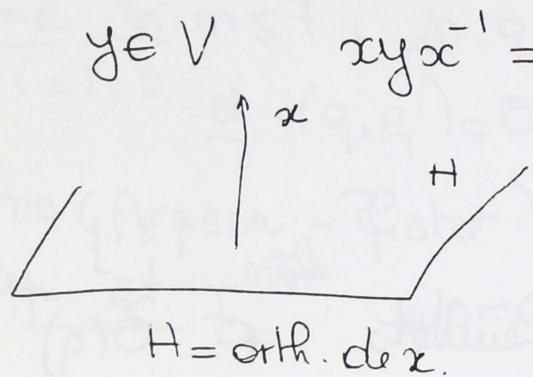
$$(x_1 \dots x_k)^t = x_k \dots x_1 \quad x_i \in V$$

Remarque

(51)

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

$$x = x^{-1}$$



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

$$xyx = -xxy = -y.$$

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

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

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

C^+ eng. par les produits pairs

$$x_1 \dots x_n \quad x_i \in V$$

$$C^- \quad \text{impairs}$$

C^+ pair / C^- impair

$$\tilde{\mathbf{O}}(q) = \{z \in C^+, z z^1 = 1, z V z^{-1} = V\} = \tilde{\mathbf{O}}(q)_+$$

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

K Groupes algébriques sur K

$$\tilde{\mathbf{O}}(q)_+, \dots, (\tilde{\mathbf{O}} = \tilde{\mathbf{O}}_+ \cup \tilde{\mathbf{O}}_-)$$

Ces groupes ont les propriétés voulues

A définir

$$\tilde{\mathbf{O}}(q)_+ \rightarrow \mathrm{SO}(q)$$

$$\begin{smallmatrix} \downarrow \\ z \end{smallmatrix}$$

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

$$\tilde{\mathbf{O}}(q)_- \rightarrow \mathrm{O}(q) - \mathrm{SO}(q) \quad v \mapsto -z v z^{-1}$$

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

comme si c'était exacte de groupes algébriques

(pas exact bien sûr sur le corps de base!).

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

Si l'on a des vecteurs de carrés 1 pour q , on en choisit un, $O(q) = SO(q) \times (1, \sigma)$ σ réflex. l'hyp perpend.

$$\tilde{O}(q) = Spur(q) \times (1, \sigma)$$

(Bruno Kahn)

I Formes de Pfister

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2$$

$$(x_1^2 + \dots + x_4^2)(y_1^2 + \dots + y_4^2) = (x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4)^2 + \dots$$

N polynôme homogène de degré d en n var /F, car \mathbb{F} est

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

(1) E/F extension $N(E^n) - \{0\}$ est un sous-grou.ex: $N = \Sigma$ de 2 \square , 4 \square , 8 \square Si $E = F(x_1, \dots, x_m, y_1, \dots, y_m)$ (2) formule $N(\vec{x})N(\vec{y}) = N(\vec{\phi}(x, y))$
avec $\vec{\phi}(\vec{x}, \vec{y}) \in E$.

(fractions rationnelles)

Rq: L'inverse est facile! $N(x)^{-1} = \frac{N(x)^{d-1}}{N(x)^d}$ et par homogénéité $= N\left(\frac{x}{N(x)}\right)$ Si $\vec{\phi}$ peut être donné par des polynômes, alors $N = N_0$
avec

$$N_0 = N_{E/F} \circ N_{\mathbb{D} \text{ corps}}$$

 $[\mathbb{F} : F] \subset \mathbb{D}$ corps gauche
de centre

ou

$$N_0 = N_{E/F} \circ \nu_0$$

 $[\mathbb{E} : F] \subset \mathbb{D}$ "corps" d'octonions
de centre E , ν_0 nommé
de \mathbb{D} .
Il n'y a rien d'autre: $\vec{\phi}$ donné par des polyn. homog.
d'où donné par loi d'algèbre, si tordue convenable
avec éléments à gche et drte; c'est forcément altern.
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.

La notation \otimes signifie qu'il existe des lois littérales.

Théorème (Pfister) φ forme quadratique anisotrope
cond. équiv.

- (1) EIF extension $\varphi(E^n)$ de φ est un gpe
- (2) φ est multiplicative avec $\varphi(\vec{x})\varphi(\vec{y}) = \varphi(\vec{\phi}(\vec{x}, \vec{y}))$
- (3) $\vec{\phi}$ 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 .

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

\downarrow
W espace
vect ss jacent
 $\ominus \varphi_{n-1}$

$$V = W \oplus W^\perp$$

φ_{n-1} forme de Pfister donc multiplicative
 $\forall x \in V$ $\exists v_x \in GL(W)$ $\varphi_{n-1} \circ v_x = \varphi_{n-1}(x) \varphi$

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

$$x = \underset{W}{x_0} + \underset{W}{x_1} \quad u_x = \begin{pmatrix} v_{x_0} & a_n v_{x_1} \\ v_{x_1}^* & w \end{pmatrix} \quad v? \in Einf_U$$

$v_{x_1}^*$ adjoint

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

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

$$v = u_{x_1}^{-1} u_{x_0}^* u_{x_1} \quad \text{det } u_{x_1} = \varphi_{n-1}(x_1)^2$$

$$\text{dén } v_x = (\det u_{x_1})^{2^{n-1}} \det(u_{x_0}) \det(u_{x_0})^{n-2} \varphi_{n-1}(x_0)^2$$

Pour 16 variables par exemple:

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

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

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

$\Delta(F)$ = plus petit nombre de \square nécessaires

Corollaire $\Delta(F)$ est une puissance de 2.

$$\text{Dém } -1 = x_1^2 + \dots + x_s^2 \quad \Delta = \Delta(F)$$

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

$$2^m \leq \Delta < 2^{n+1}$$

$$\underbrace{x_1^2 + \dots + x_{2^n}^2}_a + \underbrace{x_{2^n+1}^2 + \dots + x_s^2}_b + 1 = 0$$

Notation φ forme quadratique

$$\mathcal{D}_F(\varphi) = \{ \varphi(x) \mid x \in F^n \} - \{ 0 \}$$

ici a et b sont représentés par $\varphi: \mathcal{D}_F(x_1^2 + \dots + x_{2^n}^2) \ni$

\mathcal{D}_F est un groupe

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

Théorie des formes de Pfister

(56)

Prop : I_F^m est engendré adolūt par les m formes de Pfister.

$I_F =$ idéal de l'anneau de Witt tq concept du noyau de l'augmentation

 $= \text{Ker} (W(F) \xrightarrow{\text{rg}} \mathbb{Z}/2\mathbb{Z})$

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

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

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

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

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

Corps de fonctions, de rang N

q forme quadratique $\forall N \geq 3$ ou $N=2$ et q anisotrope

X_q = variété des zéros de q affine

projective

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

$$\text{dim } F(q) = N-1$$

(cas projectif $N-2$)

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

$$q = \langle 1 \rangle \perp -q'_{x_1, \dots, x_n}$$

$$F(q) = F(x_1, \dots, x_n, \sqrt{q(x_1, \dots, x_n)})$$

ie extension quadratique d'une trans. pure

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

$F(q) \cap F$ est transversale $\Leftrightarrow q$ isotrope sur F

$$\Leftrightarrow q = xy \perp ?$$

\Rightarrow Lemme q anisotrope $\cap F$
 $q \otimes_F F(q)$ est anisotrope.

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

Lemme 1 $E = F(\sqrt{a})$

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

$$\text{Ker}(W(F) \rightarrow W(E)) = \text{Ker } W$$

q anisotrope $\cap E$ isotrope $\Rightarrow q \geq \overbrace{2}^{\text{contient une forme}}$

contient une forme.

$$\varphi > \varphi \Rightarrow \exists \psi, \text{ tq } \psi \simeq \varphi \perp \varphi,$$

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

Si $\psi(\vec{x}) \in \mathcal{D}_{F(\vec{x})}(\varphi)$, alors $\psi > \varphi$.

Théorème φ, ψ deux formes quad., ψ anisotrope
dum $\varphi > 1$

Hypothèse: $\psi \otimes_F F(\varphi)$ 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 $\text{Ker}(W(F) \rightarrow W(F(\varphi))) = \varphi W(F)$.

Démonstration

58

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

$$\varphi \otimes_F F(\varphi) = \varphi \otimes_{F(x_2, \dots, x_n)} F(x_2, \dots, x_n, \sqrt{\varphi(x_1, \dots, x_n)})$$

hyperbolique

$$\Rightarrow \varphi'(x_2, \dots, x_n) \in \mathcal{D}_{F(x_2, \dots, x_n)}(\varphi)$$

$$\varphi \underset{F(x_2, \dots, x_n)}{\sim} \varphi'(x_2, \dots, x_n) \gg \otimes \emptyset$$

$$\Rightarrow \varphi^*(x_1, x_2, \dots, x_n) \cdot \varphi = \varphi \text{ sur } F(x_1, x_2, \dots, x_n)$$

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

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

$$a \varphi(x_1, \dots, x_n) \in \mathcal{D}_{F(x_1, \dots, x_n)}(\varphi) \Rightarrow \varphi > a \varphi$$

Théorème d'Arason-Pfister (~ 1971)

q forme quadratique de rang $< 2^m$

On suppose que $[q] \in I^n F$

Alors q est hyperbolique.

Notation $q \sim q' : \exists R_1, R_2 \quad q \perp R_1 \simeq q' \perp R_2$
hyperboliques.

$$q \sim \varepsilon_1 \varphi_1 + \dots + \varepsilon_r \varphi_r \quad \varepsilon_i = \pm 1 \quad \varphi_i \text{ formes de Pfister}$$

On raisonne par récurrence sur r.

Si φ_r non hyp., φ_r anisotrope

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

Si q non hyp., $q_{an} = \varphi_r \otimes ? \Rightarrow \text{rg } q_{an} \geq 2^m$ ercl

Invariant cohomologique

(59)

$$a_1, \dots, a_n \in F^* \mapsto \{a_1, \dots, a_n\} \in k_n F = K_n^m F / \mathbb{Z}$$

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

Corollaire $(a_1, \dots, a_n) \in H^m F = H^m(F, \mathbb{Z}/2)$ me 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 de H^1 via Kummer
 \cup cup produit.

Démonstration

$$\langle\langle a_1, \dots, a_n \rangle\rangle \simeq \langle b_1, \dots, b_n \rangle$$

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 $\forall c \in F^*$ rq $\varphi = \langle\langle a_1, \dots, a_{n-1}, c \rangle\rangle = \langle\langle b_1, \dots, b_{n-1}, c \rangle\rangle$
D'où:

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

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

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

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

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

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

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

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

(60)

Dém du 2^e lemme pour $n=2$

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

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

$$0 \quad (\text{relation de Steinberg})$$

Dém. du lemme d'Arason

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

$$= 1 \perp \varphi'_1$$

$$\varphi_2 = \langle\langle b_1, \dots, b_{n-1} \rangle\rangle$$

$$= 1 \perp \varphi'_2$$

Hypothèse $\varphi_1 \otimes \langle\langle a_n \rangle\rangle \perp -\varphi_2 \langle\langle b_n \rangle\rangle$ 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 $\leq N$, $\rho < \Theta$
 $\text{rg } \rho > N \Rightarrow \rho$ est isotrope.

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

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

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

$$\begin{array}{ccc} & \mathbb{I}_F^m / \mathbb{I}_F^{m+1} & \\ \mathbb{F}_m F & \nearrow & \downarrow e_F^m \\ \{ a_1, \dots, a_n \} & \searrow & H^m F \\ & (a_1, \dots, a_n) & \end{array}$$

Arason (Elman - Lam)

 $\varphi_1, \varphi_2, \varphi_3$ formes de Pfister

$$\varphi_1 \perp \varphi_2 \equiv \varphi_3 \pmod{\mathbb{I}_F^{m+1}}$$

$$\Rightarrow e_F^m(\varphi_1) + e_F^m(\varphi_2) = e_F^m(\varphi_3)$$

Thme (Arason) e_F^3 est bien définie VF

Thme (Jacobs-Rost, Shmeinsky) e_F^4 idem

Remarque (Milnor)

$$W_{2^{n-1}}(\langle\langle a_1, \dots, a_n \rangle\rangle') = \underbrace{(-1)^{2^{n-1} \cdot n}}_{-1 \text{ dans } H} e_F^n(\langle\langle a_1, \dots, a_n \rangle\rangle)$$

Arason montre que e_F^n est bien définie VF si VF

φ forme quadratique de rang $\geq 2^n$ $H^n F \subset H^n F(\varphi)$

$n=1$ $H^1 F \not\subset H^1 F(\varphi)$ si F n'est pas algébriquement fermé dans $F(\varphi)$
 $\rightarrow \text{rg } \varphi = 2$.

$n=2$ $\alpha \in \text{Ker}(H^2 F \rightarrow H^2 F(\varphi)) - \{0\}$

$$\alpha = [D] \quad D_{F(\varphi)} \sim 0$$

Mais $F(\varphi)$ est une extension transcendante pure de F .

$\Rightarrow D$ est un corps de quaternions $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})$

$$(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \sim 0 \Rightarrow \langle\langle a, b \rangle\rangle_{F(\varphi)} \sim 0$$

$$\Rightarrow \varphi < \langle\langle a, b \rangle\rangle$$

$$\text{rg } \varphi \leq 4$$

Thme (Arason)

φ $\text{rg } \varphi > 2$, φ anisotrope
 \nexists $\alpha \in \text{Ker}(H^3 F \rightarrow H^3 F(\varphi)) - \{0\}$

(a, b, c) convenable et convertible

$$\alpha = (a, b, c) \text{ et } \alpha \varphi < \langle\langle a, b, c \rangle\rangle$$

$$\alpha \in F^* \quad (\Rightarrow \text{rg } \varphi \leq 8)$$

Thme (Jacob-Rost) formule de Pfister

$$\text{Ker} (H^4(F) \rightarrow H^4(F(\varphi))) = e_F^4 \varphi \cup H^0 F$$

Suffit à montrer l'existence de e_F^4

Conjecture de Kato:

$$\begin{matrix} F & K_m^M F / m \rightarrow H^m(F, \mu_m^{\otimes m}) \\ (m, \text{car } F) = 1 \end{matrix}$$

$m=1$ théorie de Kummer

$m > 1$ cup produit

C'est un isomorphisme

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

Cas connus

Thme (Merkurjev-Suslin) C'est un isomorphisme

$\underline{\text{si }} n=2$

Thme (Rost-Merkurjev-Suslin)

C'est un isomorphisme

$\underline{\text{si }} n=3 \text{ et } m=2$

Thme (?) Rost: idem avec $n=4$ et $m=2^r$
(non réduite).

11/12/91.

(63)

$O(q)$

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

$$1 \rightarrow \text{Spin}(q) \rightarrow \tilde{O}(q) \rightarrow \begin{cases} \mathbb{Z}_2 & \text{si } m \geq 2 \\ 1 & \text{si } m = 1 \end{cases} \rightarrow 1$$

ext. centrale (non triviale) par $\begin{cases} \mathbb{Z}_2 & \text{si } m \geq 2 \\ 1 & \text{si } m = 1 \end{cases}$

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

$\tilde{O}(q)$ gpe algébrique

pts sur K

$C(q)$ = algèbre de Clifford

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

$x \mapsto x'$ anti-involution $x \in C^+ \Rightarrow x' \in C^-$

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

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

Il est possible bien sûr que ceci soit vide sur K

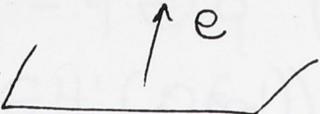
Cas $n=1$

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

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

$$1 \rightarrow \text{Spin} \rightarrow \tilde{O} \rightarrow \{\pm 1\} \rightarrow 1$$

Si K assez grand (en fait, si $\alpha = \square$ ds K),
il y a des pts rationnels de \tilde{O} se projetant sur -1.

cas
symétrie: 

(64)

Dans ce cas $\hat{O}(q)$ groupe de type $(2,2)$ formé de pts rotinuels $|_K$.

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

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

Ex: Faire tout ceci explicitement...

$$\begin{array}{ll} w_1 & q \text{ forme quadratique} \\ w_2 & n \geq 1 \text{ rang} \\ & \alpha \in H^1(K, O(q)) \end{array}$$

q_α forme tordue par α .

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

$$\begin{array}{c} O(q) \xrightarrow{\text{der}} \{ \pm 1 \} \rightarrow 1 \\ \alpha \in H^1(K, O(q)) \xrightarrow{\quad} H^1(K, \{ \pm 1 \}) = H^1(K) \\ \xrightarrow{\quad} \delta_1^\alpha(\alpha) \in H^1(K) \end{array}$$

D'autre part, suite exacte des groupes algébriques:

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

$$\Delta: H^1(K, O(q)) \xrightarrow{\quad} H^2(K) \quad \text{cordon}.$$

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

Théorème

$$\omega_1(q_\alpha) = w_1(q) + \delta'(\alpha)$$

$$\omega_2(q_\alpha) = w_2(q) + w_1(q) \cdot \delta'(\alpha) + \delta^2(\alpha)$$

On envoie $1 + \omega_1(q_\alpha) + \omega_2(q_\alpha) + \dots \equiv (1 + w_1(q) + \dots)(1 + \delta'(\alpha))$
mod termes de degré 3

Si classe de cohomol. est de $\text{SO}(q)$, la formule se simplifie ... (et se trouve dans la littérature)

Corollaire Si $q = \text{forme } \langle 1, \dots, 1 \rangle$

$$\omega_1(q_\alpha) = \delta'(\alpha), \quad \omega_2(q_\alpha) = \delta^2(\alpha).$$

Démonstration Si formule vraie pour 2 formes quadratiques, vraie par somme directe;
• vraie en dim 1.

? Vraie en dim 1: $\omega_2(q_\alpha) = \omega_2(q) = 0$.

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

$$q = \alpha x^2 \quad w_1(q) = (\alpha) \in H^1(K)$$

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

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

$$1 \rightarrow \pm 1 \rightarrow \tilde{0} \rightarrow \pm 1 \rightarrow 1, \text{ d'où}$$

$$H^1(K) \rightarrow H^1(K, \tilde{0}) \rightarrow H^1(K) \xrightarrow{\Delta} H^2(K)$$

L'action de Galois sur $\tilde{0}$ est attachée au caractère (α) .

On a déjà trouvé une formule donnant le cohomol. dans le cas d'une telle action, à partir de la suite avec action tri-nielle $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$. C'est celle qu'on veut !

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

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

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

$$\alpha = \alpha' + \alpha'' \in H^1(\mathcal{O}(q))$$

en utilisant $\mathcal{O}(q') \times \mathcal{O}(q'') \hookrightarrow \mathcal{O}(q)$.

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

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

Comme très, la 1^{re} est évidente. Pour le 2^e

$$\hat{\mathcal{O}}(q) \times \hat{\mathcal{O}}(q'') \xrightarrow{\quad} \mathcal{O}(q) \quad (\Delta \text{ pas injectif!})$$

\downarrow

$$\mathcal{O}(q) \times \mathcal{O}(q'') \hookrightarrow \mathcal{O}(q) \quad (\text{mais pb du produit})$$

$\hat{\mathcal{O}}(q') \hookrightarrow \hat{\mathcal{O}}(q)$

$\hat{\mathcal{O}}(q'') \hookrightarrow \hat{\mathcal{O}}(q)$

\downarrow

Si $g \in \hat{\mathcal{O}} \rightarrow \mathcal{O} \xrightarrow{\text{def}} (\pm 1)$

$\varepsilon(g) = \pm 1$ image de ± 1

Si g et g' est de $\hat{\mathcal{O}}(q'), \hat{\mathcal{O}}(q'')$ avec l'un des 2 pairs ils commutent; si les 2 sont impairs, ils anticommutent.

(se voit par exemple sur les symétries).

Calcul du cobord.

$$\delta^2(\alpha) \quad \alpha' \text{ repr. par } s \mapsto a'_s \in \mathcal{O}(q')$$

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

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

$$(s, t) \mapsto b'_s \cdot b'_t \cdot b_{st}^{-1} \in \{ \pm 1 \}_q$$

$$\alpha'' \quad a''_s, b''_s \quad a_s = (a'_s, a''_s) \in \mathcal{O}(q' \oplus q'')$$

$$b_s = b'_s \cdot b''_s \quad (\text{le produit étant calculé dans } \hat{\mathcal{O}}(q))$$

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

$$\cdot b_{st}^{-1} \cdot b_{st}^{-1}$$

$$\varepsilon(b''_s) \in \mathbb{Z}/2\mathbb{Z}$$

(67)

$$(s, t) \mapsto (-1)^{\varepsilon(b''_s) \varepsilon(b'_t)} b'_s \wedge b'_t (b''_s b''_t b''_{st}) \cdot b''_{st}$$

" cobord de
ds le centre

$$u, v', \cancel{v''}$$

$$\text{avec } u = (-1)^{\varepsilon(b''_s) \varepsilon(b'_t)}$$

$$v' = b'_s \wedge b'_t b'_{st}^{-1}$$

$$v'' = b''_s \wedge b''_t b''_{st}^{-1}$$

$$\varepsilon(b''_s) = \varepsilon(a''_s) \text{ et } \varepsilon(b'_t) = \varepsilon(a'_t)$$

d'où la formule voulue.

Fin de la démonstration du thm. sur la torsion

Réurrence sur $m = \text{rang}$.

Vrai si $m = 1$.

$m \geq 2$ on choisit une décomposition $q = q' \oplus q''$
avec $\text{rang } q' > 0$ et $\text{rang } q'' > 0$.

Or: $H^1(O(q') \times O(q'')) \rightarrow H^1(O(q))$ est surjectif.

Plus généralement (ε_i) base orthogonale de q

$$(\pm 1)^m \hookrightarrow O(q).$$

$$O(1) \times \dots \times O(1)$$

et $H^1(\downarrow (\pm 1)^m) \rightarrow H^1(O(q))$ est surjectif

$$\alpha = (\alpha_1, \dots, \alpha_n) \in K^*/K^{*2}$$

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

$$q_\alpha = \langle \alpha_1 \alpha_1, \dots, \alpha_n \alpha_n \rangle$$

on trouve donc tout !

Octaques de Cayley

$e_0 = 1$

$e_i \in \mathbb{Z} \bmod 7$

$e_1 \mapsto \pm e_1$

$e_2 \mapsto \pm e_2$ fixe le reste

$e_3 \mapsto \pm e_3$

$H^1(K, (\pm 1)^3) \rightarrow H^1(K, G_2)$
surjectif.

(Les 3 formes de G_2 sont classées par les 3 formes de Pfister que l'on attrape avec le "petit" groupe.)On peut supposer $\alpha = \alpha' \perp \alpha''$

d'où $Q_\alpha = Q_{\alpha'} \oplus Q_{\alpha''}$

$w(Q_\alpha) = w(Q_{\alpha'}) \cdot w(Q_{\alpha''})$

$\equiv w(Q') \cdot (1 + \delta^1(\alpha') + \delta^2(\alpha'))$

$\cdot w(Q'') \cdot (1 + \delta^1(\alpha'') + \delta^2(\alpha'')) \pmod{\text{deg } 3}$

$w(Q_\alpha) \equiv w(Q) (1 + \delta^1(\alpha) + \delta^2(\alpha)) \dots$

d'où le thme.

Remarques sur le caractéristique 2

On s'intéresse à une forme quadratique "non dégénérée" (donne quadrique lisse)

 $\text{disc} \neq 0$ (si disc bien défini).En dim paire sur K alg clos
impaire

$x_1 x_2 + \dots + x_{2m-1} x_{2m}$

$x_0^2 + x_1 x_2 + \dots + x_{2m-1} x_{2m}$

On va attacher à ces formes des invariants

$m = 2m \quad \alpha(Q)$ lisse

composante neutre $S(Q)$

$1 \rightarrow S(Q) \rightarrow O(Q) \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$

invariant
de Dickson

$$\text{Si } \alpha \in H^1(\mathcal{O}(q)) \rightarrow \delta^1(\alpha) \in H^1(\mathbb{Z}/2\mathbb{Z}) = K/\mathbb{Z}K$$

(69)

$\beta x = x^2 + x \text{ en car 2.}$

définit l'invariant d'Arf des H^1 , à partir de la forme standard

Inv d'Arf trivial :

$$1 \rightarrow \mu_2 \rightarrow \text{Spin}(q) \rightarrow \text{SO}(q) \rightarrow 1$$

~~Ce revêtement n'a pas topo. étole ne donne pas ce qu'on veut~~

$$\alpha \in H^1(K, \text{SO}(q)) \rightarrow \delta^2 \alpha \in H^2_{\text{fppf}}(\mu_2) \simeq \text{Br}_2(K)$$

En dimension paire, alors les formes s'obtiennent comme

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 + \alpha_4 x_4^2 + \dots$$

$$\text{et } \delta^2 \alpha = \sum [\alpha_i, \beta_i] \in \text{Br}_2(K) \text{ (à renfler)}$$

$$n = 2m+1$$

$\mathcal{O}(q)$ pas lisse

$$1 \rightarrow \text{SO}(q) \rightarrow \mathcal{O}(q) \xrightarrow{\det} \mu_2 \rightarrow 1$$

lisse

$$\text{en fait: } \mathcal{O}(q) = \mu_2 \times \text{SO}(q).$$

$$\alpha \in H^1_{\text{fppf}}(\mathcal{O}(q))$$

$$\det \alpha = \delta^1(\alpha) \in H^1_{\text{fppf}}(\mu_2) = K^*/K^{*2}$$

$$\delta^2(\alpha) \in \text{Br}_2(K).$$

car $K \neq 2$

$$H^1(\text{SO}(q)) \xrightarrow{\alpha} H^1(\mathcal{O}(q)) \text{ injective } (n \geq 1)$$

$$1 \rightarrow \text{SO} \rightarrow 0 \rightarrow \pm 1 \rightarrow 1$$

$$\mathcal{O}(q)(K) \xrightarrow{\text{det}} \{ \pm 1 \} \rightarrow H^1(\text{SO}(q)) \xrightarrow{\alpha} H^1(\mathcal{O}(q))$$

$O(q)(K) \xrightarrow{\pm 1}$ surjective (réflexions déterminant -1). (70)

$\alpha^{-1}(1) = \{1\}$ "injectivité naïve" (ce n'est pas des groupes!).

Par torsion

$$H^1(SO(q)) \xrightarrow{\text{injectif}} H^1(O(q)).$$

$$H^1(K, \text{Spin}(q))$$



$$H^1(KSO(q))$$

on note $H^1(K, SO(q))_{\text{spin}}$ l'image de cette flèche

Sont $\alpha \in H^1(O(q))$, $\alpha \in H^1(SO(q)) \Leftrightarrow \delta^1(\alpha) = 0$.

$$\alpha \in H^1(SO(q))_{\text{spin}} \Leftrightarrow \begin{cases} \delta^1(\alpha) = 0 \\ \delta^2(\alpha) = 0 \end{cases}$$

$$w_i(q_\alpha) = w_i(q) \quad i=1,2$$



α est spinoriel.

On a une flèche canonique

$$H^1(K, SO(q))_{\text{spin}} \xrightarrow{i(i=i_3)} H^3(K)$$

\Downarrow

$$Q_\alpha = q_\alpha \oplus (-q)$$

$[Q_\alpha] \in W_K$ (groupe de Witt de K)

$W \supset I$ idéal d'augmentation $\supset I^2$

$W/I \cong \mathbb{Z}/2\mathbb{Z}$ (\hookrightarrow rg des formes mod 2).

$$I/I^2 \cong H^1(K)$$

$$Q_\alpha \rightarrow 0 \text{ ds } \mathbb{I}/\mathbb{I}^2$$

$$\mathbb{I}^2/\mathbb{I}^3 \simeq H^2(K) \text{ (Metzner-Suslin)}$$

La classe étant spinorielle, les w coïncident, d'où
 $Q_\alpha \in \mathbb{I}^3$.

$$\mathbb{I}^3/\mathbb{I}^4 \simeq H^3(K) \text{ (Röf, M.S.)}$$

$$\text{On note se fait en fait } \mathbb{I}^3_{K^4} \longrightarrow H^3(K)$$

$$\text{D'où } [Q_\alpha] \longrightarrow i_3(\alpha) \in H^3(K).$$

Si $i_3(\alpha) = 0$, alors on peut définir α_4 dans $H^4(K)$.

L'invariant i_3 :

- Si on remplace q par λq , $\lambda \in K^*$, alors $i_3(\alpha)$ ne change pas. En effet $O(\lambda q)$, $SO(\lambda q)$, $H^1(K, SO(\lambda q))_{\text{spin}}$ et resp. $O(q)$, $SO(q)$, $H^1(K, SO(q))_{\text{spin}}$

$$Q_\alpha = q_\alpha \oplus -q$$

$$\lambda Q_\alpha = \lambda q_\alpha \oplus -\lambda q$$

$$\text{Si } Q \in \mathbb{I}^n, \quad \lambda Q \equiv Q \pmod{\mathbb{I}^{n+1}}$$

$$\text{car } \lambda Q - Q = (\lambda - 1) Q \text{ et } \lambda - 1 \in \mathbb{I}.$$

- $i_3(\alpha_1 \perp \alpha_2) = i_3(\alpha_1) + i_3(\alpha_2)$

$$\alpha_1 \in H^1(K, SO(q_1))_{\text{spin}}$$

$$\alpha_2 \in \underline{\quad}$$

$$\alpha_1 + \alpha_2 \in H^1(K, SO(q_1 + q_2))_{\text{spin}}$$

$$Q_{\alpha_1 \perp \alpha_2} = Q_{\alpha_1} \oplus Q_{\alpha_2}$$

$$i_3(\alpha_1 \otimes \alpha_2) = i_3(\alpha_1) \operatorname{rang}(\alpha_2) + i_3(\alpha_2) \operatorname{rang}(\alpha_1)$$

72

Démonstration: $[q_{\alpha_1}] \neq q_1 + \varepsilon \quad \varepsilon \in I^3$

$$i_3(\alpha) = \text{classe de } q_{\alpha} - q \pmod{I^4}$$

$$q_{\alpha_1} \otimes q_{\alpha_2} = q_1 \otimes q_2 + q_1 \otimes \varepsilon + q_2 \otimes \varepsilon + \varepsilon \varepsilon$$

On décompose q_1 en somme: $q_1 \otimes \varepsilon = \underbrace{\varepsilon_1 + \dots + \varepsilon_n}_{\text{mod } I^4} \quad \text{10 } q_1 \text{ fois.}$

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 gps non orthogonaux, par exemple exceptionnels

$G \begin{cases} G_2 & \text{pas d'automorph. externe} \\ F_4 & \text{pas de centre!} \\ E_8 & \end{cases}$

G sur K abst simple

$G \simeq \operatorname{Aut} G$

- Les représentations irréductibles $\overset{de G}{\sim} V$ sont "réalisables" sur K .
Après extension, poids dominant ω
 V_{ω} unit $\longleftrightarrow \omega$

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 $G \longrightarrow \operatorname{SO}(q_{\omega})$ (car G connexe).

Groupes connexes, donc à relèves

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \mathrm{Spin}(0/\omega) \\ & \xrightarrow{\quad} & \downarrow \\ & & \mathrm{P}\omega \rightarrow \mathrm{SO}(q\omega) \end{array}$$

Si $\alpha \in H^1(K, G)$, ρ_ω^α est spinorelle, d'où un $i_3(\rho_\omega^\alpha)$
Ne dépend pas de $q\omega$

D'où pour tout poids dominant ω et tout
 $\alpha \in H^1(K, G)$, un élé $i_\omega(\alpha) \in H^3(K)$

Exemple $G = G_2$

Partons de la forme déployée

$$\omega = a\omega_1 + b\omega_2 \quad a, b \in \mathbb{N}$$

ω_1, ω_2 représentations de \mathfrak{f} et \mathfrak{f}_4 respect.

(Octonions de trace 0) (rep. adjointe).

$$\omega = \omega_1 : H^1(K, G_2) \hookrightarrow H^3(K)$$

image formée des éléments décomposables $(a)(b)(c)$, $(a), (b), (c) \in H^1(K)$.

description par les 3 formes de Pfister

A démontrer: $i_{a\omega_1 + b\omega_2}(\alpha) = \begin{cases} 0 & \text{dépôt de } a \text{ et } b \\ i(\alpha) = i_{\omega_1}(\alpha) & \end{cases}$

Ex: $i_{\omega_2}(\alpha) \neq 0$, i.e forme de Killing
 $Ki\omega_2 - Ki\mathfrak{p} \in I^4$

$$\text{Abres } i_4(Ki\omega_2 - Ki\mathfrak{p}) \stackrel{?}{=} (-3) \cdot i(\omega)$$

$$Ki\omega_2 = \langle 1, -3 \rangle \otimes \varphi_7$$

$$1 \oplus \varphi_7 = \varphi_8 \text{ (octonions)}$$

et que $i_p(\alpha) \in H^3$

$i: R(G) \rightarrow H^3(K)$

anneau des repr.

$$i(p_1 \oplus p_2) = i(p_1) + i(p_2)$$

$$i(p_1 \otimes p_2) = i(p_1) \text{rg} p_2 + i(p_2) \text{rg}(p_1)$$

$V_{\omega_1}, V_{\omega_2}$ engendrent $R(G_2)$, donc suffisant de connaître représent explicité .. (voir p. 111 bis)

18 février 1991

(75)

G_2, F_4, E_8 ss, simplement connexe
 $\text{Aut } G \simeq G$

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

$H^1(K, G) \rightarrow H^3(K)$ $i_3(\rho, \alpha)$

$f: G \xrightarrow{\text{Spin}} SO$, on choisit une f.q. invariante.
 $\alpha \in H^1$

On a: $H^1(K, G) \rightarrow H^1(K, SO)_{\text{spin}} \xrightarrow{i_3} H^3(K)$.

Repr. irrédu. de G_2 dépendent de 2
paramètres m, n .

Le foncteur i_3 s'étend à toutes les r
représentations de G . car $K = 0$

Soit ρ une repr. lin. de V .

$V \simeq \bigoplus_{S \text{ irred}} S \otimes W_S$

W_S en.
de dim $< \infty$
act. triv. de G .

$$W_S = \text{Hom}^G(S, V)$$

q invariante sur V

S irred.

q_S f. quad. inv. sur S

$$q = \bigoplus q_S \otimes \phi_S$$

ϕ_S : forme quadratique non dég. sur W_S
ne compte que mod 2

On pose $i_3(\rho, \alpha) = \sum_S \overline{\dim W_S} \cdot i_3(\rho_S, \alpha)$
 $\in H^3(K)$

A voir :

clerk aussi le i_3 associé à

$$H^1(K, G) \rightarrow H^1(K, SO(V, q))$$

$$\downarrow \\ H^3(K)$$

DS $W(K)$

$$n_S = \dim W_S$$

$$(q_S \otimes \phi_S)_2 - (q_S \otimes \phi_S) = (q_S \otimes n_S)_2 - (q_S \otimes n_S)$$

$$(\text{mod } I^4)$$

$$\text{ou } q_S \otimes n_S = q_S \oplus \cdots \oplus q_S.$$

$$\underbrace{(q_s^2 - q_s)}_{\in \mathbb{L}^3} \otimes \underbrace{(\phi_s - \eta_s)}_{\in \mathbb{L}} \in \mathbb{L}^4$$

$$i_3(p_1 \oplus p_2) = i_3(p_1) + i_3(p_2)$$

$$i_3(p_1 \otimes p_2) = i_3(p_1) \text{rang}(p_2) + i_3(p_2) \text{rang}(p_1)$$

et fin!

$$i_3(\alpha) : R(G) \rightarrow H^3(K).$$

déterminé par ses valeurs sur des générateurs de $R(G)$, par exemple sur les représentations "fondamentales" p_1, \dots, p_ℓ correspondant aux poids fondamentaux w_1, \dots, w_ℓ .

Le cas de G_2

$$G = G_2 \quad \text{déployé}$$

$\alpha \in H^1(K, G_2)$, d'où G_α tordu

C_α algèbre d'octonions

forme norme φ_α (3-forme de Pfister)

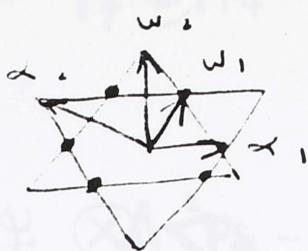
Inversement, toute 3-forme de Pfister définit un α et un seul. On a :

$$i_3(\varphi_\alpha) \in H^3(K).$$

Deux représentations fondamentales.

(78)

Poids et racines :



① dim 7 poids 0 et les 6 racines courtes

Trace 0 dans alg. d'octonions

Forme quadratique: la norme $N = \varphi$.

Forme quadratique: la norme $N = \varphi$.
 $\varphi \simeq \underbrace{\langle 1, \alpha, \beta, \gamma, \alpha\beta, \alpha\gamma, \beta\gamma \rangle}_{\varphi_7}$

$$\varphi \simeq \langle 1 \rangle \oplus \varphi_7$$

Forme quadratique: la norme $N = \varphi$
 sur les éléments de trace 0, i.e. φ_7 .

$$\varphi_7^\alpha - \varphi_7 = \varphi^\alpha - \varphi \quad (\varphi^\alpha = \langle 1 \rangle \oplus \varphi_7^\alpha)$$

Donc le i associé à cette repr. est
 celui que l'on connaît déjà.

② dim 14

représentation 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 déplié

$$W = \underline{h} \oplus (\text{orthogonal})$$

$$\begin{array}{c} x_\alpha, x-\alpha \\ \hline \text{hyperbolique} \end{array}$$

$$\langle 1, 3 \rangle \simeq x^2 + x_4 + y^2$$

$$\varphi_7 \simeq -1 \text{ dans } W(K)$$

D'où le théorème dans le cas déplié.

[En caract. 3, cette forme est dégénérée.]

La repr. de dim 14 est réductible en caract. 3 : somme de 2 repr. de dim 7.]

λ - structure : puissances extérieures

$$q \mapsto \wedge^i q \text{ défini sur } \text{Gr } W.$$

$$\Lambda^2 P_7 \cong P_7 \oplus P_{14}$$

(dim 21 = 7 + 14)

$$P_{14} \longrightarrow \Lambda^2 P_7 \quad \text{et} \quad \Lambda^2 P_7 \longrightarrow \Lambda^2 V$$

$$\Lambda^2 P_7 \longrightarrow P_7$$

$x \wedge y \mapsto \pi(xy - yx)$ sur élé. de trace 0.
en fait, $\pi(xy)$ suffit.

On a $\Lambda^2 P_7 \cong P_7 \oplus P_{14}$. Donc:

$$\begin{array}{ccc} \downarrow & & \downarrow \text{K.ell} \\ \varphi_7 & & \end{array}$$

$$\Lambda^2 \varphi_7 \cong \lambda \varphi_7 + \mu \text{K.ell} \quad \lambda, \mu \in \mathbb{Q}^\times$$

(i.e. les deux ch. lin.)

$$\varphi_7 \cong \langle \alpha, \beta, \gamma, \dots \rangle$$

$$\lambda^2 \varphi_7 \cong \langle \alpha\beta, \alpha\gamma, \dots \rangle$$

21 prod. =

On constate que:

$$\lambda^2 \varphi_7 \cong \varphi_7 \oplus \varphi_7 \oplus \varphi_7$$

Plus généralement:
Si Ψ est une n -forme de Pfister, alors et si on pose:

$$\Psi = \Psi - \langle 1 \rangle, \text{ alors } \lambda^2 \Psi = (2^{n-1} \bigcirc \Psi)$$

$$\langle 1, 1, 1 \rangle \otimes \varphi_7 \simeq \lambda \varphi_7 + \mu \text{Kill}$$

disc, $\text{Kill} = 3$ car vrai cas déployé

$$\text{disc } \varphi_7 = 1$$

On trouve $\lambda = 3$ (à un carré près)

$$\langle 3 \rangle \varphi_7$$

$$\text{Calcul de } \mu = ?$$

$$g : \text{Kill} \hookrightarrow \Lambda^2 \mathfrak{p}_7$$

" o (7 variables)

Sur l'alg. de Lie d'un groupe orth. on a la forme trace $\text{Tr}(xy)$. Et:

$\text{Kill} = 4$. forme trace

(dans le cas déployé se voit sur les poids)

$$\text{Lie}(\underline{\text{SO}}) \simeq \Lambda^2 V \quad \text{On a } \begin{cases} \text{Tr} \\ \Lambda^2 q \end{cases}$$

$$\text{Trace} : -2 \times \Lambda^2 q$$

$$\text{Sur } \underline{\text{SO}} \simeq \Lambda^2 V \quad \text{donné par}$$

V ev. avec forme bilin. sym.

$$\Lambda^2 V \rightarrow \underline{\text{SO}}(V)$$

$$v_1 \wedge v_2 \mapsto (x \mapsto B(v_1, x)v_2 - B(v_2, x)v_1)$$

$$\text{Disc} : \mu = -2$$

$$\text{D'où } \langle -2 \rangle_{\text{Kill}} \oplus \langle \cancel{3} \cancel{4} \rangle \cong \langle 1, 1, 1 \rangle \otimes \varphi_7 \\ \langle 1, 1, 1 \rangle = \langle 3, 2, 6 \rangle \cong \langle \cancel{1}, \cancel{6} \rangle \otimes \varphi_7$$

$$\text{Res } K_{\text{Kill}} \cong \langle -1, -3 \rangle \otimes \varphi_7$$

$$K_{\text{Kill}} \cong \langle -1, -3 \rangle \otimes \varphi_7^\alpha$$

$$K_{\text{Kill}} \cong K_{\text{Kill}} = \langle -1 \rangle \otimes \underbrace{\langle 1, 3 \rangle}_{\in I} \otimes \underbrace{(\varphi_7^\alpha - \varphi_7)}_{(\varphi^\alpha - \varphi)} \\ (\varphi = \varphi_5)$$

C'est dans I^4 . Donc:

$$i_4(\alpha) \in H^4(K)$$

$$i_4(\alpha) = (-3) i_3(\alpha) \in H^4(K)$$

$$i_3(\alpha, \rho_4) = 0.$$

Consequence

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 $\omega = n_1 \omega_1 + n_2 \omega_2$, comment

Calculer explicitement $i_3(\rho, \alpha)$? (Voir p. 111 bis.)

Pour cela, il faut écrire V_w comme polynôme en P_1 et P_2 .

Complément 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:

$$N(x) = x_0^2 + \alpha x_1^2 + \beta x_2^2 + \gamma x_3^2 + \dots + \alpha \beta x_4^2 + \dots$$

C alg. d'octonions

Posons: $N(x) + \delta N(y) = \Phi$.

C'est une forme à 16 variables, 4-forme de

Pfister. Formule:

$$(N(x) + \delta N(y)) \cdot (N(z) + \delta N(t)) = N(x\bar{z} + \delta y\bar{t}) + \delta N(xt - xz, x^{-1}y\bar{t})$$

$x, y, z, t \in \mathbb{C}$

$$x^{-1} = \bar{x}/N(x).$$

(2) A-t-on $i_3(\alpha) = 0$ pour tout α (et tt β)
(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. adjoint)
forme de Killing, signature

$i_3 \in H^3(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. Il y a 3 possibilités:

-5/2	compacte
4	dejloyée
= 20	

$n_+ - n_-$

F_4 repr. fond. en dim. 26

J Alg. de Jordan except. de dim 27

repr. fond. = élém. de trace 0 dans J .

$$\text{Aut } J = F_4$$

Forme $\text{Tr}(\alpha y)$ 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 O , et d'une forme hermitienne à 3 variables sur $O \rightarrow 3$ scalaires, $\gamma_1, \gamma_2, \gamma_3 \in K^*$. Autrement dit, J est formée des

matrices 3×3 , à coeff. de O , hermitiennes

$$\text{par rap. } \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ 0 & \gamma_2 & \gamma_3 \\ 0 & 0 & \gamma_3 \end{pmatrix} = \Gamma \quad (A\Gamma = \Gamma^t \bar{A})$$

$$J = \begin{pmatrix} x_1 & c_3 & c_2 \\ \lambda_3 \bar{c}_3 & x_2 & c_1 \\ \lambda_2 \bar{c}_2 & \lambda_1 \bar{c}_1 & x_3 \end{pmatrix} \quad \begin{array}{l} \text{où } x_i \in K, c_i \in C \\ \text{et } \lambda_1 = \gamma_3/\gamma_2, \lambda_2 = \gamma_3/\gamma_1, \lambda_3 = \gamma_2/\gamma_1 \end{array}$$

$$H^1(K, F_4)_{\text{red}} \subset H^1(K, F_4)$$

15
classes de J
(réduites)

J détermine l'algèbre d'octonions 0 (85)

3 - forme de Pfister Ψ_8

5 - forme de Pfister $\Psi_{32} = \Psi_8 \otimes \Psi_4$ où

$$\Psi_4 = \langle 1, \gamma_1^{-1}\gamma_2, \gamma_2^{-1}\gamma_3, \gamma_3^{-1}\gamma_1 \rangle.$$

J est déterminé à isom. près par

Ψ_8, Ψ_{32} que l'on peut se donner

arbitrairement

En effet, Ψ_8 et $\Psi_{32} \iff$ forme trace de J

(Springer)

Conj. de Milnor \Rightarrow les alg. de Jordan réduites sont définies par

$$\begin{cases} x_3 \in H^3(K) \\ x_5 \in H^5(K) \end{cases} \text{ avec les conditions}$$

① x_3 est décomposable

② $x_5 \in x_3 \cdot H^2(K)_{\text{dec}}$

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 toute à l'heure

$$\text{La forme trace est } Q_J = 2(x_1^2 + x_2^2 + x_3^2) + \bar{\gamma}_1 \bar{\gamma}_2 N(c_3) + \dots + \bar{\gamma}_2^{-1} \bar{\gamma}_3 N(c_2).$$

$$\text{i.e. } Q_J = \langle 2, 2, 2 \rangle \oplus \langle \bar{\gamma}_1 \bar{\gamma}_2, \bar{\gamma}_2 \bar{\gamma}_3, \bar{\gamma}_3 \bar{\gamma}_2 \rangle \otimes N.$$

La connaissance de Q_J détermine à la fois la 3-forme de Pfister N et la 5-forme de Pfister $N \otimes \langle 1, \bar{\gamma}_1 \bar{\gamma}_2 \rangle$.

$$\text{On a } N \in \mathbb{I}^3, \quad \gamma N \in \mathbb{I}^3, \quad \gamma N \equiv N \pmod{\mathbb{I}^4}$$

$$Q_J - \langle 2, 2, 2 \rangle \equiv N \pmod{\mathbb{I}^4}.$$

Or, si (N, N') sont des 3-formes de Pfister, on a $N \equiv N' \pmod{\mathbb{I}^4} \Rightarrow N \simeq N'$.

$$\text{5-forme} = Q_J - \langle 2, 2, 2 \rangle \oplus N.$$

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 $N \simeq N'$.

$$N = \langle 1 \rangle \oplus \Phi_7, \quad N' = \langle 1 \rangle \oplus \Phi'_7$$

$\Phi_7 \simeq \Phi'_7$. On choisit $\alpha \neq 0$ tel que

$-\alpha$ est représenté par Φ_7 et Φ'_7 .

D'où $e_1 \in C$, $\text{Tr } e_1 = 0$, $e_1^2 = -\varphi_7(e_1) = \alpha$

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 $\varphi_6 = \varphi - \langle e_1, \alpha \rangle$ et de même φ_6' .

Par Witt: $\varphi_6 \cong \varphi_6'$

Il existe $(-\beta \neq 0)$ représenté par φ_6, φ_6' .

D'où $\left| \begin{array}{l} e_2 \in C, \quad e_2 \perp (1, e_1), \quad e_2^2 = \beta \\ e_2' \in C' \end{array} \right. \quad e_2'^2 = \beta$

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 (est déterminée par celle de K_2 , $e_2^2 = \beta$, $e_2 \perp (1, e_1)$. (Voir plus loin)

K_4 de dim. 4

Sur 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: $c, d \in K_4$ $e_3^2 = \gamma$

$$(a + b e_3) (c + d e_3) = a c + \gamma \bar{d} b + (d a - b \bar{c}) e_3$$

(Autre façon (T.5)) -

V de dim. 8, q de disc. 1
inv. de Witt trivial

V', V'' repr.
semi-spinorielles

$V \otimes V'$ fait intervenir
 V'' , etc.

On normalise un système de racines de longueur
1, soit e, e_1, e'' . On identifie V, V', V''
(formes isom.) Loi de produit des rac.

SO_3 opér. sur V, V', V''

$(x, y, \mapsto xy)$

$\subset \cong \text{Alg. ocl}$

$(g \in \text{Spin } \subset)$

Revenir aux généralités sur les $f \cdot q$.

théorème d'injectivité du H^1

Thm de Witt: $q = q' \oplus q''$

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

donne $H^1(K, O(q')) \hookrightarrow H^1(K, O(q))$

② Pfister

$$q = q' \otimes q''$$

$$\mathcal{O}(q') \longrightarrow \mathcal{O}(q)$$

$$x \mapsto x \otimes 1$$

Th Si rang q'' est impair, l'application

$$H^1(K, \mathcal{O}(q')) \rightarrow H^1(K, \mathcal{O}(q))$$

est injective

③

Th (Springer)

Si K'/K est une ext. de degré impair,
alors la flèche naturelle

$$H^1(K, \mathcal{O}(q)) \rightarrow H^1(K', \mathcal{O}(q)) \text{ est injective}$$

$$\parallel$$

$$H^1(K, \mathcal{O}(q)) \rightarrow H^1(K, R_{K'/K} \mathcal{O}(q))$$

② \Rightarrow ③

(D'abord, énoncés en termes de f. q.)

K'/K extension. $f: K'/K \rightarrow f^* q: K \rightarrow K'$. On

se donne $\lambda: K' \rightarrow K$, K -forme linéaire $\neq 0$

$\Psi: f^* q$ sur $V'/K' \mapsto x \mapsto \lambda(\Psi(x))$,
 $f^* q$ sur V'/K

$\Psi \mapsto \Psi_\lambda$

(cas part. $\mathcal{N} = x^2$ sur K' , $n = [K':K]$)

90

ψ_λ forme : $x \in K' \mapsto \lambda(x^2) = q_\lambda(x)$ (n variables).

$$\psi = \sum_{i=1}^r \alpha_i x_i^2 , \quad \alpha_i \in K^*$$

$$\psi_\lambda \simeq \sum \alpha_i \lambda(x_i^2) \simeq \langle \alpha_1, \dots, \alpha_r \rangle \otimes q_\lambda$$

$$\psi_\lambda \equiv \psi \otimes q_\lambda$$

Autre faç. de voir :

$$\mathcal{O}(q) \rightarrow R_{K'/K} \mathcal{O}(q) \rightarrow \mathcal{O}(q \otimes q_\lambda)$$

—

$\mathcal{O}(q)$, repr. \mathfrak{f}

conditions générales sur \mathfrak{f} pour obtenir
injectivité au niveau des H^1 ? On ne sait pas ...

car $K \neq 2$ ① Théorème de simplification de Witt

$$H^1(K, O(q)) \rightarrow H^1(K, O(q \otimes q'))$$

est injectif

② (Arason - Pfister) même énoncé avec $q \otimes q'$, et
rang q' impair.③ (Springer) K'/K de degré impair

$$H^1(K, O(q)) \rightarrow H^1(K', O(q))$$

est injectif

"

$$H^1(K, R_{K'/K} O(q))$$

② \Rightarrow ③ faitDémonstration de ②Il suffit de montrer que $q \mapsto q \otimes q'$ définit
une injection

$$W_K \longrightarrow W_K$$

② \Leftrightarrow (q') dans W_K est non diviseur de
 q' est de rang impair $\Leftrightarrow q' \notin I$

$$W_K / I \cong \mathbb{Z} / 2\mathbb{Z} \quad (\text{rang})$$

Lemme: $\cap I^n = 0$ dans W_K Supposons que l.o.l. Alors il y aurait une
f.g.Q anisotrope de rang ≥ 1 , $t \cdot q$.
 $(Q) \in I^n$ pour tout n .

Impossible si $\text{rang}(Q) < 2$.
 q' est inversible mod tout I' .

(92)

On voudrait avoir un critère, étant donné

$$\varphi: O(q) \rightarrow O(Q)$$

critère pour l'injectivité sur le H^1 ?

Par exemple, puissances extérieures?

① On peut supposer q' de rang 1.

$$q' = \langle \alpha \rangle, \alpha \in K^*$$

Il suffit de démontrer que le noyau est 0.

$G_1 \subset G_2$ groupes algébriques

$$\text{Ker: } H^1(K, G_1) \rightarrow H^1(K, G_2) = ?$$

$$1 \rightarrow H^0(G_1) \rightarrow H^0(G_2) \rightarrow \underbrace{H^0(G_2/G_1)}_{X} \rightarrow$$

$$\rightarrow H^1(G_1) \rightarrow H^1(G_2)$$

Le noyau est donc

$X(K)/G_2(K)$: ensemble des
 orbites de $G_2(K)$
 dans $X(K)$.

Injectivité $\Leftrightarrow G_1(K)$ opère transitivement sur les points rationnels de l'espace homogène $X = G_2/G_1$.

Ici $X = \widetilde{O(q+q')}/O_q$

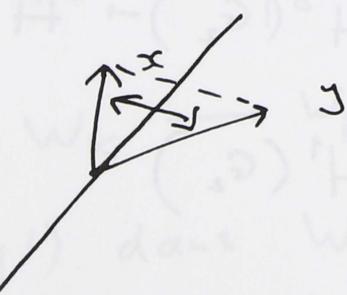
$$O_{n+1}^Q/O_n$$

113

Sphère des $x \in K^{n+1}$ avec $Q(x) = d$.

Quadrique affine. On a 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 :

$O_n \hookrightarrow O_{nm}$ n impair de $SO_{nm}(K)$
 montrer directement que l'action sur les points rationnels de O_{nm}/O_n est transitive ??

③ (Springer) 2 variantes de démonstration

a) démonstration de Schur

$\lambda: K' \rightarrow K$ forme linéaire non nulle
 $n = [K': K]$ $\lambda \mapsto q_\lambda$ de rang n
 $q_\lambda(x) = \lambda(x^2)$.

$W_K \xrightarrow{i} W_{K'}, \xrightarrow{\lambda} W_\lambda$

$\lambda \circ (q) = q \otimes q_\lambda$

Il existe des choix de λ qui sont
tel que $(q_\lambda) \simeq \langle 1 \rangle$ dans W_K .

Choix de λ :

Supposons d'abord que K' soit une extension normale de K . Soit $t \in K'$

tel que $K' = K(t)$

K' base $1, t, \dots, t^{n-1}$.

$$\lambda(1) = 1 \quad \lambda(t^i) = 0, \quad 1 \leq i \leq n-1.$$

Lemma $-q_\lambda \simeq \langle 1 \rangle \oplus \frac{n-1}{2} \cdot \text{forme hyperbolique}$

$$K' = K \oplus V, \quad V = Kt \oplus \cdots \oplus Kt^{\frac{n-1}{2}}$$

$$q_\lambda(x, y) = \lambda(x \cdot y)$$

$$q_\lambda = \langle 1 \rangle \oplus q_{\lambda, V}$$

$$V \text{ contient } W = Kt \oplus \cdots \oplus Kt^{\frac{n-1}{2}}$$

$$W \cdot W \subset V, \quad \lambda(w \cdot w) = 0$$

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 λ

$$K' \supset K'' \supset K$$

$\xrightarrow{\lambda} \quad \xrightarrow{\lambda''}$

$$\lambda = \lambda'' \circ \lambda'$$

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 :

$$q \text{ anisotrope sur } K \Rightarrow q \text{ anisotrope sur } K'$$

Entraine l'honneur précédent.

Vrai en caract 2 aussi, avec la même démonstration.

Démonstration :

On peut supposer K'/K monogène,
 $K' = K[t]/(p(t))$ p unitaire, irréductible
 de degré n

Récurvance sur n .

$x = (x_1, \dots, x_N)$ N variables.

$q(x'_1, \dots, x'_N) = 0$ $x'_i \in K'$ non tous nuls.

$x'_i = \alpha_i(t)$ $d^\circ \alpha_i \leq n-1$, α_i sans facteur commun

$q(\alpha_1(t), \dots, \alpha_N(t)) \equiv 0 \pmod{p(t)}$

$Q(t)$ de degré ?

Soit r le maximum des degrés des α_i .

$\alpha_i = \alpha_i^r t^r + \dots + \alpha_i^0$ avec α_i^r non tous nuls.

$$Q = q(\alpha_1 t^r + \dots, \alpha_2 t^r + \dots, \dots, \alpha_N t^r + \dots)$$

$$= t^{2r} q(\alpha_1, \dots, \alpha_N) + \text{polynôme de degré } \\ \text{a- plus } 2r-1$$

q est anisotrope : $q(\alpha_1, \dots, \alpha_N) \neq 0$.

Donc degré de $Q = 2r \leq 2n-2$

$$Q = p Q' \quad \deg Q' = 2r - h$$

$$\leq n-2$$

impair

Soit p' un facteur irréductible de degré impair de Q' .

$$Q \equiv 0 \pmod{p'}$$

et $(t) \neq \text{sous } p'$ tous $0 \pmod{p'}$.

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 $q_2 \iff q_1 \oplus (-q_2)$
contient r_2 fois la forme $h = \langle 1, -1 \rangle$

$$\begin{aligned} \Rightarrow q_1 &= q_2 \oplus q_3 & q_1 \oplus (-q_2) &= q_2 \oplus (-q_2) \oplus q_3 \\ & & \langle \alpha \rangle \oplus \langle -\alpha \rangle &\cong \langle 1, -1 \rangle. \\ & & &\cong r_2 h \oplus q_3 \end{aligned}$$

$$\begin{aligned} \Leftarrow q_1 \oplus -q_2 &= r_2 h \oplus q_3 \\ &= q_2 \oplus (-q_2) \oplus q_3 \end{aligned}$$

$\Rightarrow q_1 \cong q_2 \oplus q_3$ par Witt.

On est donc ramené à prouver que
 si: q contient n fois h sur K' ,
 q contient m fois h sur K .

$$Q = Q_{\text{ans}} + x \cdot h \quad x \geq n \quad /k$$

$$x \geq m \quad /k$$

② q forme quadratique $/k$

S: q est une n -forme de Pfister sur K
alors — " — sur K

$$\text{rang } q = 2^m = N$$

q n -forme de Pfister \Leftrightarrow q est hyperbolique
 ou q aniso, et
 il existe z_1, \dots, z_N
 $\in K(x, y)$

telles que

$$q(x) q(y) = q(z).$$

on bien q est hyperbolique $/k'$
 donc sur K

on bien des $z_i \in K'(x, y)$ existent avec
 $q(x) q(y) = q(z')$.

q représente $q(x) q(y)$ sur $K'(x, y) = K' \otimes_K K$
 de degré impair sur $K(x, y)$

$q(x)q(y) \in k(x,y)$ est représenté

sur $k'(x,y)$, donc sur $k(x,y)$

$m = 1, 2, 3, \dots$

q m -forme de Plücker \Leftrightarrow q représenté
invariants de q

$H: (k) \rightarrow H'(k')$ injectif.

donc H^1, H^2, \dots
 H^{m-1} sont 0

Questions.

$w_k \rightarrow w_{k'}$ est injectif

$k_m^M K \rightarrow I_k^m / I_k^{m+1}$

\downarrow
 $H^m(K)$

conj : isom.

on passe à K' \rightarrow diagramme

$H^m(K) \rightarrow H^m(K')$ injectif

a) $k_n^M K \rightarrow k_n^M K'$ injectif ?

oui : Bass-Tate, Katō
(trace) \downarrow
LN 342, p. 379, corollary

b

$$I_K^m / I_K^{m+1} \rightarrow I_{K'}^m / I_{K'}^{m+1}$$

injectif

Oui : car le transfert $I_K^m \rightarrow I_K^m$

(J.K.) $\xrightarrow{\text{Arason}}$

voir aussi les 2 lignes
du haut de la p. 465

←

Formes trace ; cas des algébres
centrales simples.

car $K \neq \mathbb{F}_2$

A algèbre simple centrale sur K
de rang $= 2$

$$[A] \in \text{Br}(K)$$

$\text{Tr}_d = \text{trace réduite de } A$

$$q_A(x) = \text{Tr}_d(x^2)$$

forme bilinéaire correspondante ($= \frac{1}{2}$ associé)

est $\text{Tr}_d(xy)$

cas déployé : $A = M_n(K)$

$$\text{Tr}_d(x) = \text{Tr}(x) \quad x \in M_n(K) \quad , \quad x = (x_{ij})$$

$$\text{Tr}(x^2) = \sum x_{ii}^2 + 2 \sum_{i < j} x_{ij} x_{ji} \quad \text{D'où :}$$

$$q_A^{\text{def}} = \underbrace{\langle 1, \dots, 1 \rangle}_n + \frac{n(n-1)}{2} h \quad h = \langle 1, -1 \rangle.$$

On va comparer q_A et q_A^{dec} .

1^{er} cas: "impair"

$$\text{Alors } q_A \simeq q_A^{\text{dec}}$$

En effet, il existe K'/K de degré

impair q' décompose A .

Donc $(*)$ est vraie sur $K' \Rightarrow$ vraie sur K

(grâce au théorème de Springer). Voici une application:

Thm (Wedderburn): car $K \neq \mathbb{Z}$

Si $n = 3$, A est une algèbre cyclique

$[A] \in \text{Br}_3(K)$ peut s'écrire

$$[A] = x \cdot y, \quad x \in H^1(K, \mu_3)$$

$$y \in H^1(K, \mathbb{Z}/3\mathbb{Z})$$



A contient un corps cubique cyclique car $K \neq \mathbb{Z}$

A monter: il existe $\alpha \in A$ avec

$$\alpha^3 \in K^* \text{ et } \text{Trd}(\alpha) = 0, \quad \text{Trd}(\alpha^2) = 0.$$

sol. corad. $t^3 - x$

Soit V espace vdr. de dim 8, $\text{Trd}(\alpha) = 0$.

$q_A | V$ forme de rang 8

$q_A | V$ représente 0. Sinon,

q_A = anisotrope de rg 8 $\oplus \langle \wedge \rangle$.

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

opérant 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 $y \in H^1(L, \mathbb{Z}/3\mathbb{Z})$.

$H^1(K, \mathbb{Z}/3\mathbb{Z})$

$(\text{rest. } \mu_3) \stackrel{\downarrow}{=} \text{points fixes de l'involution agissant sur:}$

$H^1(L, \mathbb{Z}/3\mathbb{Z})$,

[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.

$$[A] = x y^+ + x y^-, \quad (\text{invariant}) \quad [A] = [A^+]$$

$x = x^+$

$$[A] = x y^+$$

donc: $y^+ \in H^1(K, \mathbb{Z}/3\mathbb{Z})$, et l'on a
 $[A] = x y^+$, c.q.f.d.

En fait, pour \mathfrak{p} premier et A algèbre centrale simple de rang \mathfrak{p}^2 , A est cyclique $\Leftrightarrow A^*$ contient α , $\alpha \in K$, $\alpha \mathfrak{p} \in K$

autrement dit, $A \supset K(\sqrt[p]{x})$
 $x \in K^*$.

Remarque —

$$\mathfrak{p} = 3 \quad \alpha^3 \in K^*, \quad \alpha \notin K$$

$x \mapsto \alpha x \alpha^{-1}$ automorphisme de A d'ordre 3.

Suffisant de trouver un sous-corps commutatif maximal de A , stable par σ , mais pas fixe par τ .

$\text{PGL}(A)$ groupe alg. plusieurs très maximaux stables, ??

cas 2 :

à résoudre $\text{Tr } a = 0$, $\text{Tr } a^2 = (\text{Tr } a)^2 = 0$
 sol. après ext. de degré impair
 → 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

$$w_1(q_A) = w_1(q_A^{\text{dec}}) = n_2(-1) \in H^1(K)$$

$$q_A^{\text{dec}} = n \langle 1 \rangle \oplus \dots \bar{n}_2 h \quad \text{où } h = \langle 1, -1 \rangle$$

$$\text{et } n_2 = \frac{n(n-1)}{2}.$$

Théorème

$$w_2(q_A) = w_2(q_A^{\text{dec}}) + \frac{n}{2} [A].$$

$$[A] \in \text{Br}_n(K) \quad \text{et} \quad n[A] = 0, \text{ donc}$$

$$\frac{n}{2} [A] \in \text{Br}_2(K).$$

$$A = (A^{\text{dec}})_{\alpha},$$

$$\alpha \in H^1(K, \text{PGL}_n)$$

$$A^{\text{dec}} = M_n$$

$$\mathrm{PGL}_n = \mathrm{Aut}(A^{\mathrm{dec}})$$

A^{dec} est un espace vec. mun: de la forme quadratique $q_A^{\mathrm{dec}} = (\mathrm{Tr}(xy))$

Tout automorphisme de A^{dec} respecte q_A^{dec}

$$\mathrm{PGL}_n \xrightarrow{\varphi} \mathrm{O}(q_A^{\mathrm{dec}}) \quad (\text{un}^2 \text{ var.})$$

$$\mathrm{Aut}(A^{\mathrm{dec}})$$

$$H^1(K, \mathrm{PGL}_n) \xrightarrow{\cong} H^1(K, \mathrm{O}(q_A^{\mathrm{dec}})) \quad (\gamma = \varphi(\varphi))$$

Foncteur algèbre simple centrale \rightarrow espace quadr.

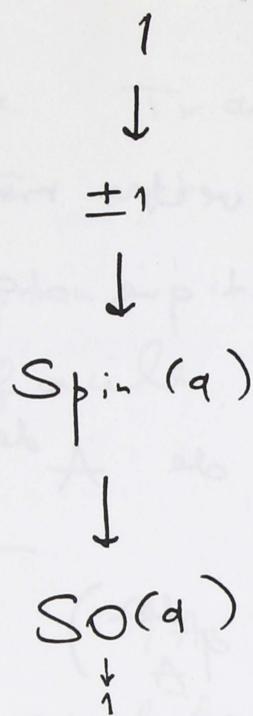
q_A est la bordure de q_A^{dec} par

$$\gamma \in H^1(K, \mathrm{O}(q^{\mathrm{dec}}))$$

$$\begin{aligned} \delta^1: H^1(K, \mathrm{O}(q)) &\rightarrow H^1(K, \mathbb{Z}/2\mathbb{Z}) \\ 1 &\rightarrow \mathrm{SO}(q) \rightarrow \mathrm{O}(q) \rightarrow \{\pm 1\} \rightarrow 1 \end{aligned}$$

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

Par connexité, l'image de PGL_n ds $\mathrm{O}(q^{\mathrm{dec}})$ est contenue dans $\mathrm{SO}(q^{\mathrm{dec}}) \Rightarrow \delta^1 = 0$.



$$\delta^2: H^1(\text{SO}(q)) \rightarrow H^2(K, \mathbb{Z}/2\mathbb{Z})$$

$$w_2(q_{\beta}) = w_2(q) + \delta^2(\beta)$$

$$\beta \in H^1(K, \text{SO}(q))$$

$$\begin{array}{ccc}
 M_n & \xrightarrow{\quad} & M_2 \\
 \downarrow & & \downarrow \\
 \text{SL}_n & \xrightarrow{\quad} & \text{Spin}(q_A^{\text{dec}}) \\
 \downarrow & & \downarrow \\
 \text{PGL}_n & \xrightarrow{\quad \psi \quad} & \text{SO}(q_A^{\text{dec}})
 \end{array}$$

car SL_n est simplement connexe.

$$\nu(\beta) = \left\{ \begin{array}{l} 1 \\ \beta^{n/2} \end{array} \right.$$

$$\nu(\beta) = \beta^{n/2}$$

Lemme :

Donc ν est surjectif.

admettons le lemme pour le moment.

$$\alpha \in H^1(K, PGL_n) \rightarrow H^2(K, \mu_n) = Br_n(K)$$

$\downarrow \cong$ \downarrow

$$H^1(K, SO) \longrightarrow H^2(K, \mu_2)$$

L'image de α dans $Br_n(K)$ est $-[A]$

$$\frac{n}{2}(-[A]) = \frac{n}{2}[A].$$

$$\text{D'où } \delta^2(\beta) = \frac{n}{2}[A]$$

et la formule en résulte.

[Si car divise n , il faut prendre la cohomologie plate.]

Il reste à prouver le lemme:

si φ non surjectif $\Rightarrow \varphi = 1$

la flèche $SL_n \rightarrow \text{Spin} \xrightarrow{\sim} \overline{\varphi}$
se factoriserait en $PGL_n \rightarrow \text{Spin}$

φ se relèverait en $\tilde{\varphi}$.

$$PGL_n \dashrightarrow \text{Spin}^{n^2} \qquad \text{à voir que non.}$$

$$PGL_n \rightarrow SO_{n^2}$$

Technique connue en th. des groupes alg.
pour voir si une repr. se relève aux spinors.

G réductif connexe, \mathfrak{g} représentation
orthogonale de G .

On choisit un tore maximal T .

Poids de ρ (écrits additionnellement)

poids 0 multiplicité quelconque

paires $(\omega_i, -\omega_i)_{i \in I}$ avec même multiplicité, $\omega_i \neq 0$.

On forme alors $\sum_{i \in I} \omega_i$; le résultat est :

$$\sum_{i \in I} \omega_i = 0 \pmod{2} \text{ dans } X(+)$$

(les ω_i sont répétés suivant leurs multiplicités)



ρ spinorelle

Remarquons que $-\frac{\omega_1}{2} + \dots + \frac{\omega_n}{2} = \frac{\omega_1 + \dots + \omega_n}{2} - \omega_1$

Ici, on a :

$GL_n \rightarrow PGL_n$ e_1, \dots, e_n poids de repr. évidente de GL_n .

Groupe des poids de PGL_n est l'ensemble

des $m_1 e_1 + \dots + m_n e_n$ avec $m_i \in \mathbb{Z}$ et

$$m_1 + \dots + m_n = 0$$

(il est engendré par les $e_i - e_j$).

Les poids de PGL_n agissent sur M_n par autom. int. soient les $e_i - e_j$ $i, j \in [1, n]$.

Les non nuls sont les $e_i - e_j$ ($i < j$)

et leurs opposés (mult. 1)

110 120
On forme $w = \sum_{i < j} (e_i - e_j)$ 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.

$$w = (n-1)e_1 + \dots \quad w \neq 0 \pmod{2}$$

car w est pair.

Rappel sur G_2

$$\text{car } 0 \quad \iota : H^1(K, G_2) \hookrightarrow H^3(K, \mathbb{Z}/2\mathbb{Z})$$

$$\omega = n_1 \omega_1 + n_2 \omega_2$$

$$\text{repr. } \varphi_\omega : H^1(K, G_2) \rightarrow H^1(K, SO_\omega)_{\text{sp}} \rightarrow H^3(K)$$

$$\iota_\omega : H^1(K, G_2) \rightarrow H^3(K)$$

$$\iota_\omega = \begin{cases} 0 & \omega = 0 \text{ unité ou } \omega = \omega_2 \text{ (dim 14)} \\ i & \omega = \omega_1 \text{ (repr. de dim 7)} \end{cases}$$

$$\omega \equiv \omega' \pmod{8} \Rightarrow \iota_\omega = \iota_{\omega'}$$

Pour $n_1, n_2 \leq 8$, on détermine les valeurs de ι_ω
(voir tableau, page suivante)

retour à $\text{Tr}(x^2)$

A algèbre simple centrale, $n^2 = [A : K]$

$$q_A(x) = \text{Tr}_d(x^2) \quad \text{rang } n^2$$

$$n \text{ impair} \quad q_A \approx q_A^{\text{dec}}$$

$$n \text{ pair} \quad w_1(q_A) = w_1(q_A^{\text{dec}})$$

$$w_2(q_A) = w_2(q_A^{\text{dec}}) + \frac{n}{2} [A]$$

$$q_A - q_A^{\text{dec}} \in I_K^2 \quad I_K = \text{idéal max. de } W_K$$

$$\text{cl}(q_A - q_A^{\text{dec}}) \in I_K^2 / I_K^3 \cong \text{Br}_2(K)$$

$$\frac{n}{2} [A].$$

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 ($\omega_1 \rightarrow$ repr. de dim. 7 ; $\omega_2 \rightarrow$ 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 $\varepsilon_\omega \rightarrow$

$n_1 \backslash n_2$	0	1	2	3	4	5	6	7
0	0, 0_{14}	1_{77}	1_{273}	0	0	0	0	0
1	1_7	0_{64}	0_{296}	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_{10}	0	0	0
7	0	0	0	0	0	0	0	0

(En indice : dimension de la repr., en caract. 0)

Noter $i_\omega = 0$ si $n_2 \equiv 1, 5, 7 \pmod{8}$

Cas particulier $n = 4$

$$[A] \in \mathrm{Br}_4(K), \quad \overline{[A]} = 0 : [A] \in \mathrm{Br}_2(K)$$

Alors $A = A_1 \otimes A_2$, A_1 alg. quat.

$$A_\lambda = (a_\lambda, b_\lambda) \quad \lambda = 1, 2$$

$$q_A - q_A^{\text{dec}} \in \mathbb{I}_K^3. \quad \text{Image de } \mathbb{I}_K^3 / \mathbb{I}_K^4 \cong H^3(K)$$

$$q_A = q_{A_1} \otimes q_{A_2}$$

Soit (a, b) un corps de quaternions.

Forme norme N :

$$x = x_0 + x_1 i + x_2 j + x_3 k, \quad k = ij$$

$$N(x) = x_0^2 - a x_1^2 - b x_2^2 + ab x_3^2$$

$$N_{(a,b)} = \langle 1, -a, -b, ab \rangle.$$

Forme trace:

$$x^2 = (x_0^2 + a x_1^2 + b x_2^2 - ab x_3^2) + \dots$$

$$q_{(a,b)} = 2 \langle 1, a, b, -ab \rangle$$

$$q_A = \langle 1, a_1, b_1, -a_1 b_1 \rangle \otimes \langle 1, a_2, b_2, -a_2 b_2 \rangle$$

comparer à la norme:

$$N_{ab} + \left\langle \frac{1}{2} \right\rangle q_{(a,b)} = \langle 1 \rangle + \langle 1 \rangle = 2$$

dans W_K

$$q_A = (2 - N_1) \otimes (2 - N_2) \quad N_1 = N_{a_1, b_1}, \quad N_2 = N_{a_2, b_2}.$$

$$N_A = N_{a_2, b_2} \quad q_A^{\text{dec}} = 4.$$

113

$$\begin{aligned} q_A - q_A^{\text{dec}} &= 4 - 2(N_1 + N_2) + N_1 N_2 - 4 \\ &= -2(N_1 + N_2) + N_1 N_2. \end{aligned}$$

$$2 \in I_K^2, \quad N_2 \in I_K^2, \quad \text{donc}$$

$$q_A - q_A^{\text{dec}} \in I_K^3.$$

classe dans I_K^3 / I_K^4 ?

$$2 \longrightarrow I_K / I_K^2 = H^1(K)$$

" $\langle 1 \rangle - \langle -1 \rangle$ "

$$2 \longrightarrow \langle -1 \rangle \in H^1(K).$$

$$\begin{aligned} q_A - q_A^{\text{dec}} &\longrightarrow \langle -1 \rangle (x_1 + x_2) = \langle -1 \rangle [A] \\ &\in H^3(K). \end{aligned}$$

$$x_2 = [A_2] \in H^2(K)$$

Que se passe-t-il si -1 est un carre' ds K ?
 $\langle -1 \rangle = 0$ ds $H^1(K)$.

$$2 = \langle 1 \rangle - \langle -1 \rangle = 0 \quad (\text{car } \langle 1 \rangle = \langle -1 \rangle)$$

$$2 = 0 \quad \text{dans } W_K.$$

$$q_A - q_A^{\text{dec}} = N_1 \cdot N_2 \in I_K^4$$

classe de $q_A - q_A^{\text{dec}}$ dans I_K^4 / I_K^5

114

est le cup-produit $x_1 \cdot x_2$, où $x_n = [A_n] \in H^2(K)$.

$$x = [A], \quad x = x_1 + x_2. \quad x_n = (a_n)(b_n)$$

$$\mapsto x_1 x_2 \in H^4(K).$$

ce produit ne depend 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

$$\varphi: H^2(K) \rightarrow H^4(K) \quad \text{telle que:}$$

(a) $\varphi(x+y) = \varphi(x) + \varphi(y) + xy$

(b) $\varphi(x) = 0 \quad \text{si} \quad x = a \cdot b, \quad \text{avec} \quad a, b \in H^1(K)$

Si on admet ce théorème, $\varphi(x) = x_1 x_2$ est

l'application ci-dessus.

Cartan a étudié la notion de

Puissance divisée dans les algèbres. $\binom{x^n}{n!}$

C'est un anneau commutatif, J : idéal

$$\gamma_i: J \rightarrow C \quad i = 0, 1, 2, \dots$$

$$\gamma_0(x) = 1, \quad \gamma_1(x) = x, \dots, \gamma_n(x+y) = \sum_{i+j=n} \gamma_i(x) \gamma_j(y)$$

(d'autres prop.)

$$\gamma_n(xy) = x^n \gamma_n(y) \quad y \in J \quad x \in C$$

(dans Cartan: C commutatif gradué,

\mathcal{J} : idéal des élé' de degré ≥ 1)

$$\Rightarrow n! \mathcal{J}_n(x) = x^n.$$

Exemple: k anneau commutatif
 M k -module

$$C = \bigwedge^{\text{pair}} M$$

Il y a sur C (sur les élé' > 0)

des \mathcal{J}_i uniques tels que

$$\mathcal{J}_i(x_1 \wedge \cdots \wedge x_{2n}) = 0 \quad i \geq 2, n \geq 1.$$

voir G. Papy, Thèse
~~(pas dans la thèse)~~. On le fait pour modules
 libres - sém. Cartan, puis on écrit le
 module comme quotient)

M libre de rang 2^n , $u \in \bigwedge^2 M$

$$\mathcal{P}_f(u) = \frac{u^n}{n!} \in \bigwedge^{2n} M$$

$$= \mathcal{J}_n(u)$$

K -théorie de Milnor $k^M(K)$

algèbre graduée sur \mathbb{F}_2

générateurs (x) , $x \in K^*/K^{*2} = H^1(K)$

relations $(x)(1-x) = 0$, $x \neq 0, 1 \in K$.

$$\Rightarrow (x)(-x) = 0$$

comme $-1 = \text{carre}'$, $(x)^2 = 0$

$$k^M(K) = \Lambda H^0(K)/J$$

J engendré par les $(x)(1-x)$.

(par certains élém. décomposables).

Lemma:

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 $C = (\Lambda M/J)$, (définies sur elle de degré pair), $\gamma_i(x) = 0 \quad i \geq 2$ et x décomposable.

$$x \in \Lambda^{2n} M, \quad \gamma \in \Lambda^{2n} M, \quad y \in J$$

$$\text{à vérifier: } \gamma_i(x+y) = \gamma_i(x) \pmod{J}$$

récurrence.

Montre il existe de puissances divisées sur $k^M(K)$ lorsque $-1 = \square$.

En particulier,

$$\begin{array}{ccc} \gamma: k_{2i}^M(K) & \longrightarrow & k_{2i}^M(K) \\ & & \downarrow \\ & H^{2i}(K) & H^{2i}(K) \end{array}$$

Conclusion : on a

(117)

$$\gamma_i : H^2(K) \rightarrow H^i(K)$$

$$x = \sum_{\lambda \in L} x_\lambda \quad x_\lambda \text{ décomposables} \\ \text{et ordonnées totalement}$$

$$\gamma_i(x) = \sum_{\lambda_1 < \dots < \lambda_i} x_{\lambda_1} \dots x_{\lambda_i}.$$

$i = 2$ donne $\gamma_2 = \varphi$ de tout à l'heure.

Autre façon d'obtenir φ : utiliser les puissances extrémales, Λ -structure de W_K .

A algèbre centrale simple, $n = 3$

A est cyclique, $[A] \cdot x \cdot y \in H^1(K, \mathbb{Z}/3\mathbb{Z})$
(car $K \neq 3$)

$$y \in H^1(K, \mathbb{Z}/3\mathbb{Z})$$

Remarque: ces algèbres sont classées par
 $H^1(K, PGL_3)$ sig naturel de type $(3, 3)$
(donne Heisenberg ds GL_3)

$$\begin{pmatrix} 1 & & \\ & \rho & \\ & & 1 \end{pmatrix} \quad \rho^3 = 1 \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \sigma$$

$$\rho \sigma = * \sigma \rho$$

↑ homothétie

On note:

$$\bar{\Phi} = \mu_3 \times \mathbb{Z}/3\mathbb{Z} \hookrightarrow PGL_3, \text{ sous-groupe d'ordre 9}$$

$$H^1(K, \phi) \rightarrow H^1(K, PGL_3)$$

surjective

"

$$H^1(K, \mu_3) \times H^1(K, \mathbb{Z}/3\mathbb{Z}) \ni (x, y) \mapsto$$

à vérifier : l'image de x, y dans

$$H^1(K, PGL_3) \text{ est } x \cdot y$$

?

(on - $x \cdot y$??)

$$H^2(K, \mu_3)$$

(Analogie orthogonal :

$$(\pm 1) \times \dots \times (\pm 1) \longrightarrow 0,$$

et surjectif sur H^1 .)

$n=5$: on ne sait pas si l'alg. est
toujours cyclique.

Formes traces des corps et des algèbres

étalées.

car $\neq 2$

Algèbres étalées 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

$$\sum_{n_i=1}^{\infty}, \text{ or } n_i = [E_i : K].$$

(119)

b) Après extension des scalaires, E devient isomorphe à $K \times \dots \times K$ (n fois).

c) La forme trace $q_E(xy) = \text{Tr}_{E/K}(xy)$ est non dégénérée.

Dictionnaire bre conn (Bourbaki)

K_S clôture séparable de K

$$G_K = \text{Gal}(K_S/K)$$

$$E \xrightarrow{\psi} K_S \quad K\text{-homomorphisme}$$

$$\phi_E = \text{Hom}_{K\text{-alg}}(E, K_S), |\phi_E| = n$$

action naturelle de G_K

$$s \in G_K, \varphi \in \phi_E \quad s\varphi \in \phi_E$$

action continue à gauche.

Équivalence de catégories ("th de Galois")

K -algèbres étale et ensembles finis munis
d'une action continue de G_K .
 $(G_K\text{-ensemble}).$

Structure (partielle) de q_E

$n = [E : K]$, q_E : forme de rang n

On écrit $n = 2^{m_1} + \dots + 2^{m_h}$ $m_1 < m_2 < \dots < m_h$.

1^{er} cas: $\sum m_i \equiv 0 \pmod{2}$

Alors q_E contient la forme $\langle 1, \dots, 1 \rangle$ h fois.

i.e. $q_E \cong \underbrace{\langle 1, \dots, 1 \rangle}_h + g$, g de rang $n-h$.

2^{eme} cas $\sum m_i \equiv 1 \pmod{2}$

Alors q_E contient la forme $\langle 2, 1, \dots, 1 \rangle$ h termes.

Démonstration est basée sur le thm de Springer
 E est définie par l'action de G_K sur Φ_E ,
ens. à n éléments.

À isom. près, E est déterminé par

$$\varphi_E : G_K \rightarrow S_n.$$

Classes d'algèbres étales de degré n
correspondent aux représentations galoisiennes
 $\varphi_E : G_K \rightarrow S_n$ à conj. près.

G_E = image de G_K dans $\text{Aut}(\Phi_E) \cong S_n$,
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 réiproquée de G_K , c'est $G_{K'}$, avec $[K': K]$ impair.

Par le thm de Springer, il suffit de monter la 1^{ère} étape.

1^o 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 $2^{m_1}, \dots, 2^{m_s}$ 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

$$n = 2^{a_1} + \dots + 2^{a_k} \quad \text{avec les } a_i \text{ correspondants.}$$

les a_i sont distincts.

Donc les $a_i = m_i$ à permutation près.

$$E = E_1 \times \dots \times E_l \quad \deg E_i \text{ est } 2^{m_i}$$

$$q_E = \sum q_{E_i} = \bigoplus q_{E_i}$$

$$T_{v_{E_i}}(1^2) = 2^{m_i}$$

$$q_{E_i} \cong \langle 2^{m_i} \rangle \oplus g_i \quad \text{rang } g_i = 2^{m_i} - 1$$

$$q_E \cong \langle 2^{m_1}, 2^{m_2}, \dots, 2^{m_l} \rangle \oplus g$$

$$m_i \text{ pair} \Rightarrow \langle 2^{m_i} \rangle = \langle 1 \rangle$$

$$m_i \text{ impair} \Rightarrow \langle 2^{m_i} \rangle = \langle 2 \rangle.$$

De plus $\langle 2, 2 \rangle = \langle 1, 1 \rangle$. Donc le résultat.

$$d(q_E) = \text{disc}(E) \in K^*/K^{*2} = \mathbb{H}^1(K)$$

$$n = 1, 2, 3$$

$$\underline{n = 2} \quad E = K(\sqrt{d}) \quad q_E = \langle 2 \rangle \oplus g$$

$$q_E = \langle 2 \rangle \oplus \langle 2d \rangle$$

$$\underline{n = 3} \quad q_E \cong \langle 1, 2, 2d \rangle \quad d = \text{disc}$$

Pour aller plus loin, il faut connaître

l'invariant de Witt.

$w_1, w_2 (q_E)$

123

$\varphi_E : G_K \rightarrow S_n$ défini à conjugaison près.

$H^i(S_n, \mathbb{Z}/2\mathbb{Z})$ $i = 1, 2$

$$H^1(S_n) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & n=1 \\ \mathbb{Z}/2\mathbb{Z} & n \geq 2 \end{cases}$$

$$S_n \xrightarrow{\text{sgn}} \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$$

ε_n = élément normal 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)

$$\mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z}$$

$$\varepsilon_n^2 \in H^2(S_n) \quad \downarrow \quad \downarrow$$

$$H_0 \quad \times \longrightarrow C_4$$

$$\downarrow \quad \downarrow$$

$$S_n \longrightarrow \{\pm 1\}$$

une transposition devient d'ordre 4

$$\text{Res}_H \varepsilon_n^2 \neq 0$$

$$H = \{(1), (12)\}$$

Autre élément de $H^2(S_n)$:

$$\tilde{S}_n \rightarrow \tilde{O}_n(\mathbb{C})$$

$$\downarrow \quad \downarrow$$

$$S_n \rightarrow O_n(\mathbb{C})$$

$$s_n \in H^2(S_n)$$

Dans l'extension $\tilde{S}_n \rightarrow S_n$, correspondante, une transposition reste d'ordre 2 mais le produit de 2 transpositions disjointes devient d'ordre 4.

$$S_n = 0 \quad \text{si} \quad n \leq 3.$$

$$S_n, \varepsilon_n^2 \text{ ind. } n \geq 4$$

$$H^2(S_n) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & n=2, 3 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & n \geq 4 \end{cases}$$

$n=2, 3$
base ε_n^2
base ε_n^2, s_n

Autre définition :

$$H^i(\mathcal{B}O_n(\mathbb{R})) \rightarrow H^i(S_n)$$

$$H^*(\mathcal{B}O_n(\mathbb{R})) = \mathbb{F}_2 [w_1, \dots, w_n]$$

$$w_i \mapsto \varepsilon_i \quad w_i \mapsto s_i$$

$$S_n \rightarrow O_n(\mathbb{R})$$

$$BS_n \rightarrow BO_n(\mathbb{R})$$

Démonstration de Schur:

S_n : présentation "à la Coxeter"
de type A_{n-1} $\circ - \circ - \circ - \cdots$

$n-1$ éléments d'ordre 2,

$$\sigma_1, \dots, \sigma_{n-1}$$

$$\sigma_1 = (12) \quad \sigma_2 = (23) \quad \dots \quad \sigma_{n-1} = (n-1 \ n)$$

$$\sigma_i^2 = 1, \quad \sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{si} \quad |i-j| \geq 2$$

$$(\sigma_i \sigma_j)^3 = 1. \quad (\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j)$$

$$|i-j|=1.$$

\tilde{S}_n peut être présenté par des $\tilde{\sigma}_i$, $i=1$ à n centrés

$$\text{avec} \quad \tilde{\sigma}_i^2 = 1$$

$$\tilde{\sigma}_i \tilde{\sigma}_j = -\tilde{\sigma}_j \tilde{\sigma}_i \quad |i-j| \geq 2$$

$$(\tilde{\sigma}_i \tilde{\sigma}_j)^3 = 1 \quad \text{si} \quad |i-j|=1.$$

Pour vérifier que \tilde{S}_n existe, il

utilise les spineurs.

Des \tilde{O}_n , on peut élever les symétries s_x
où $q(x)$ est un carré

Théorème (CMH, 1984)-

$$(a) \quad \omega_1(q_E) = \varphi_E^*(\varepsilon_n)$$

$$(b) \quad \omega_2(q_E) = \varphi_E^*(s_n) + (2)\omega_1(q_E)$$

$$d = \text{disc } E$$

$$\omega_1(q_E) = d$$

$$\omega_2(q_E) = \varphi_E^*(s_n) + (2)(d).$$

Démonstration par torsion galométrique

$$E^{\text{dec}} = K \times \dots \times K \quad \text{à basis}$$

$$q_E^{\text{dec}} = \langle 1, \dots, 1 \rangle \quad \text{forme unité'}$$

$$\varphi : G_K \rightarrow S_n = \text{Aut}(E^{\text{dec}})$$

φ est un 1-cocycle à valeurs dans

$\text{Aut}(E^{\text{dec}})$.

E est E^{dec} tordu par φ .

$$E = (E^{\text{dec}}) \varphi.$$

$$q_E = (q_E^{\text{dec}}) \varphi$$

$$\varphi : G_K \rightarrow S_n \subset O_n(K)$$

groupe orthogonal pour la forme unité'

$$2 q_E = (2 q_E^{\text{dec}}) \varphi$$

$$S_n \hookrightarrow O_n$$

$(i:j) \mapsto$ réflexion p.r. à $e_i - e_j$

$$q(e_i - e_j) = 2$$

$$2 q(e_i - e_j) = 4 \quad \text{corre'!}$$

$$\tilde{S}_n \hookrightarrow \tilde{O} (2 q_E^{\text{dec}}) = \tilde{\Sigma} (K)$$

$$\downarrow \quad \quad \quad \pi \downarrow \quad \quad \quad \downarrow$$

$$S_n \subset O(2 q_E^{\text{dec}}) = \Sigma (K)$$

S_n contenu dans l'image de $\tilde{\Sigma} (K)$.

Lemme:

Soit $1 \rightarrow A \rightarrow \tilde{\Sigma} \rightarrow \Sigma \rightarrow 1$

une suite exacte de groupes algébriques

A centre $\tilde{\Sigma}$, A fini, et $A(\mathbb{R}) = A(K)$

Soit \tilde{G} un s/g fini de $\tilde{\Sigma} (K)$

contenant $A = A(K)$ et soit G

son image dans $\Sigma (K)$

$$\tilde{G} \subset \tilde{\Sigma}$$

$$\downarrow \quad \quad \quad \downarrow$$

$$G \subset \Sigma$$

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 $\Delta : H^1(K, \Sigma) \rightarrow H^2(G_K, A)$,
d'où $\Delta[\varphi] \in H^2(G_K, A)$

② \tilde{G} est une extension de G par A ,
donc definit $e \in H^2(G, A)$
 $\varphi^* e \in H^2(G_K, A)$

On a: $\varphi^* e = \Delta[\varphi]$.

Rappelons la définition de Δ .

$\tilde{\alpha}_s$ relève $\alpha_s \in \Sigma(K_s)$

$$\Delta(\alpha_s)(s, t) \mapsto \tilde{\alpha}_s (\tilde{\alpha}_{st})^{-1} \tilde{\alpha}_t$$

$$\tilde{\alpha}_s \tilde{\alpha}_t (\tilde{\alpha}_{st})^{-1}.$$

ici $\alpha_s, \tilde{\alpha}_s$ sont rationnels sur K .

donc $= \tilde{\alpha}_s \tilde{\alpha}_t (\tilde{\alpha}_{st})^{-1}$.

E algèbre étale de dim n sur K

caract $K \neq 2$

$$q_E(x) = \text{Tr}_{E/K}(x^2)$$

q_E non dégénérée de rang n

$$d = \text{disc}(q_E) = \text{disc}(E)$$

$$\omega_1(q_E) = (d) \in H^1(K).$$

$$E \rightsquigarrow \varphi_E: G_K = \text{Gal}(K_S/K) \rightarrow S_n$$

defini: 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 $\omega_2(q_E) = \varphi_E^*(s_n) + (2)(d)$

$(q)_2 = q_E$, $q = q^{\text{dec}}$, forme associée à $K \times \dots \times K$

$$\varphi: G_K \xrightarrow{\varphi_E} S_n \subset O_n(K)$$

$$\omega_2(2q_E) = ?$$

$$O(2q_E^{\text{dec}}) = O(\langle 2, \dots, 2 \rangle) \leftarrow \tilde{O}(2q_E^{\text{dec}})$$

$$\sum \xleftarrow{\quad} S_n \xleftarrow{\quad} s_n \xleftarrow{\quad} \tilde{S}_n \xleftarrow{\quad} \sum$$

$$\varphi \in H^1(K, \Sigma)$$

$$1 \rightarrow c_2 \rightarrow \tilde{\Sigma} \rightarrow \Sigma \rightarrow 1$$

$$\Delta : H^1(K, \Sigma) \rightarrow H^2(K).$$

$$\text{On a : } \Delta(\alpha) = \varphi_E^*(s_n) \quad (\text{lemme})$$

Q forme quadratique, $\alpha \in H^1(K, O(Q))$

$$w_1(Q_\alpha) = w_1(Q) + \delta^1(\alpha)$$

$$w_2(Q_\alpha) = w_2(Q) + \delta^1(\alpha) w_1(Q) + \delta^2(\alpha)$$

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

$$Q = 2q^{\text{dec}}. \quad w_1(Q_\alpha) = w_1(Q) + (d)$$

$$w_1(2q) = w_1(z, \dots, z) + (d)$$

$$\text{d'où } w_1(q) = (d) \dots$$

$$w_2(2q) = w_2(2q^{\text{dec}}) + (d) w_1(2q^{\text{dec}}) + \varphi^*(s_n)$$

$$\text{Formules : } \begin{cases} w_1(\lambda q) = w_1(q) + n(\lambda) \\ w_2(\lambda q) = w_2(q) + n_1 w_1(q)(\lambda) + n_2 (-1)(\lambda) \end{cases}$$

$$\text{où } n_1 = n-1, \quad n_2 = n(n-1)/2.$$

$$d = \langle \alpha_1, \dots, \alpha_n \rangle$$

$$w_2(\langle \lambda \alpha_1, \dots, \lambda \alpha_n \rangle) = \sum_{i < j} (\alpha_i)(\alpha_j) + (\lambda)(\alpha_i) + (-1)(\alpha_i)$$

$$\lambda = 2 \quad \text{donc :}$$

$$w_2(2q) = w_2(q) + n_1(2) w_1(q)$$

$$w_2(q_E) \neq n_1(2)(d) = n(2)(d) + \varphi_E^*(s_n)$$

d'où la formule.

Bruno Kahn : formules pour les classes de Steifel-Whitney supérieures, en fonction des $\varphi_E^*(w_i(s_n))$

$S_n \rightarrow O_n(\mathbb{R})$

(131)

$w_i(S_n) \in H^i(S_n, \mathbb{Z}/2\mathbb{Z})$

$w_i(q_E)$ en fonction des $\varphi_E^*(w_i(S_n))$:

$$w = \sum w_i(q_E) = \varphi_E^*(w(S_n)) \cdot (1 + (2)(d))$$

Applications et cas particuliers :

Relèvement

$$\begin{array}{ccc} \widetilde{\varphi} & \dashrightarrow & \widetilde{S}_n \\ & & \downarrow \\ \varphi : G_K & \longrightarrow & S_n \end{array}$$

Condition de relèvement ?

$$\text{Exist. de } \widetilde{\varphi} \iff \varphi^*(S_n) = 0$$

" $w_2(q_E) + (2)(d)$

En fait, E donne explicitement

$$E = K[x]/(f(x))$$

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n.$$

On calcule $w_2(q_E)$ en fonction des coefficients.

Méthode de

Hermite - Kronecker - Klein ...

pour résoudre l'équation du 5^{ème} degré.

Que signifie "résoudre une équation" ?

(problème d'histoire des maths).

Supposons $\text{car}(K) \neq 2, 5$ (pas indispensable) 132
 As agit-il fidèlement sur une courbe de genre 0?

Vrai: sur un corps algébriquement clos
 $A_5 \hookrightarrow \text{PGL}_2(K)$, K 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 points (moins en caract. 3)

$$Y \quad g = 0$$

$$\downarrow \quad A_5$$

$$X \simeq \mathbb{P}_1$$

Une courbe de genre 0 a un invariant $\in H^2(K)$. Inv. de Y : $(-1)(-1)$.

($\sqrt{5} \in K$: chainons se A_5 , d'ordre 5)

$$A_5 \rightarrow \text{PGL}_2(K)$$

$$\text{Tr}(s^2 / \det(s))$$

$$\frac{(1+\omega)^2}{\omega} = 2 + \omega + \omega^{-1} \Rightarrow a + b\sqrt{5}$$

K quelconque.

(133)

$S: \sqrt{5} \notin K$, 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 .

$$\begin{array}{ccc}
 Y & & \\
 \downarrow & & \\
 \mathbb{P}_1/K(\sqrt{5}) & Y/A_5 & K(\sqrt{5}) \\
 \downarrow & & \downarrow \\
 \mathbb{P}_1 & Y/S_5 & K
 \end{array}$$

$$\begin{array}{ccc}
 Y_P \subset Y & & P \in Y/S_5 (K) \\
 \downarrow & \downarrow & \text{non ramifiée} \\
 P \in Y/S_5 = \mathbb{P}_1 & &
 \end{array}$$

Y_P S_5 - torsion sur K

$$\Leftrightarrow G_K \rightarrow S_5$$

\Leftrightarrow algèbre étale de dim 5 sur K

\Leftrightarrow équation de 5^{ème} degré
(à équiv. près).

"Revêtement de Klein".

Quelles sont les équations que l'on trouve ? (134)

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 TP_4 , $\sum_{i=1}^5 x_i = 0$, $\sum_{i=1}^5 x_i^2 = 0$

d'où une quadrique C dans TP_3 (hyperplan des $\sum x_i = 0$).

$Y = \text{variété des droites de la quadrique}$

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 def. $K(\sqrt{d(q)})$)

(135)

$$\langle 1, \dots, 1 \rangle = \langle 5 \rangle + \langle 5, 1, 1, 1 \rangle$$

disc. 5

$$G_K \rightarrow \{\pm 1\} \text{ associé à } K(\sqrt{5}).$$

2°) Corps des fonctions de X (méthode modulaire).D'abord sur \mathbb{Q} . Corps des fonctions modulaires de niveau 5 sur $\mathbb{Q}(\zeta_5)$ ζ_5 racine 5^{ème} de 1, appelle' K_5 .Action de $GL(2, \mathbb{F}_5)/\{\pm 1\}$.Invariants $\mathbb{Q}(\zeta)$

$$G_5 \left(\begin{array}{c} K_5 \\ | \\ (\mathbb{Q}(\zeta_5, \zeta)) \\ | \\ (\mathbb{Q}(\zeta)) \end{array} \right) \mathbb{F}_5^*$$

$$G_5 \xrightarrow{\text{det}} \mathbb{F}_5^*$$

$$\mathbb{F}_5^*/(\pm 1) \subset G_5$$

2 élé

 \mathbb{F}_5 corps des invariants,

$$\begin{array}{c} k_5 \\ | \\ G_5(\mathbb{F}_5^*/(\pm 1)) \\ | \\ \mathbb{Q}_j \end{array}$$

Donc on trouve

136

$$S_5 \left(\begin{array}{c} k_5 \\ | \\ A_5 \\ | \\ Q(\sqrt{5})(j) \\ | \\ Q(j) \end{array} \right)$$

calcul : k_5 est de genre 0.

On a donc reconstitué la situation précédente.

Les deux constructions sont isomorphes.

(Il faudrait résoudre $\sum \alpha_i = 0$, $\sum \alpha_i^2 = 0$).

car $K \neq 2, 5$, $|K|$ 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 $w_r(q_E) = (-1)(-1)$

③ Il existe $x \in E$, $x \neq 0$, avec
 $\text{Tr } x = \text{Tr } x^2 = 0$

④ Il existe $f(x) = x^5 + ax^2 + bx + c$
tel que $E \simeq K[x]/(f)$.

⑤ La forme $q_E \simeq \langle 5, 1, -1, 1, -1 \rangle$
 $= \langle 5 \rangle + \mathbb{H}$.

Extensions quadratiques:

- $\sqrt{5d}$ " irr. essentielle "
- choisir ext. quadr. faisant $\text{Tr } x=0 = \text{Tr } x^2$
et avoir un tel .
" irr. accessoire "

Brauer a vu que " irr. accessoire " était donc
par un élé de Br. .

$$E = K \cdot 1 \oplus H \quad H : \text{éléments de } \text{Tr } 0$$

$$q_E = \langle 5 \rangle \oplus q_E' \quad q_E' = q_E / H$$

$$\begin{cases} d(q_E') = 1 \\ q_E' \text{ de rang 4} \end{cases}$$

Lemma: Si Q de rang 4, $d(Q) = 1$

dans K^*/K^{*2} .

Les 3 propriétés suivantes sont équivalentes

- Q repr. 0
- $w_2(Q) = (-1, -1)$
- $Q \simeq \langle 1, -1, 1, -1 \rangle$.

$$q_E = q_E' + \langle 5 \rangle$$

$$w_2(q_E) = w_2(q_E') + (1)(5) = w_2(q_E').$$

Supposons ⑤. \mathcal{Q}_E' est alors hyperbolique (138)

$$x \neq 0 \quad T_v x = 0 = T_v x^2 = 0$$

sont les points d'une quadrique déployée / K

On veut un tel x avec $K[x] = E$ tout entier.

$$\text{Sur } \overline{K}, \quad E \sim \overline{K} \times \dots \times \overline{K}.$$

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 $\begin{matrix} Y \\ \downarrow \\ X \end{matrix}$
est un rev. gal. fini étale,

$\begin{matrix} G \\ \downarrow \\ K \end{matrix} \xrightarrow{\varphi} G$ alg. gal.

À quelle condition φ provient-il d'un point rationnel de X ?

Recette la variété Y_φ (tordue de Y
par φ) a un point rationnel,

et l'image de ce point dans $X(K)$ (139)
convexe.

On se donne $\varphi: G_K \rightarrow S_r$, on trov Y
par φ . Pt rationnel ?

$Y^{\text{dec}} = \text{variete' des droites de la quadrique}$

$$Tr x = Tr x^2 = 0.$$

(moins points rampe's)

$Y_\varphi = \text{variete' des droites de la quadrique}$

$$Tr_E x = Tr_E x^2 = 0.$$

Point rationnel dessus ?

Critere (3) -

On peut essayer d'aller plus loin: controle
sur invariants supérieurs.

E avec $w_1(q_E) = 0$ d'carre' $\varphi_E: G_K \rightarrow A_n$
 $w_2(q_E) = 0$ φ_E relevable dans \tilde{A}_n

On a une forme quadratique q_E avec

q_E et $q_E^{\text{dec}} = \langle 1, \dots, 1 \rangle$ mèmes w_1, w_2

$$q_E - q_E^{\text{dec}} \in I_K^3 \rightarrow H^3(K)$$

$i_3(E) = \text{image de } \varphi_E - \langle 1, \dots, 1 \rangle$
dans $H^3(K)$.

(140)

Calculer $i_3(E)$?

Premier cas intéressant : $n=6$.

$$\varphi_E : G_K \rightarrow \tilde{A}_6$$

$H^i(\tilde{A}_6, \mathbb{Z}/2\mathbb{Z})$ = cohérence 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 ?)

(Nakao ~ 1950)

Soit u la classe non triviale de $H^3(\tilde{A}_6)$

$$\varphi : G_K \rightarrow \tilde{A}_6$$

$$\varphi^* u \in H^3(K).$$

Est-ce que $i_3(E) = \varphi^*(u)$?

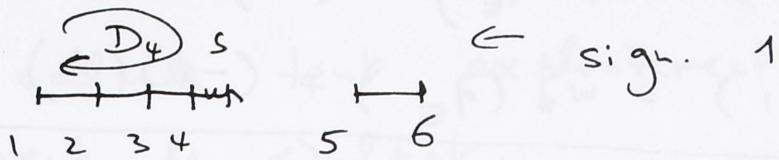
Vrai si $\sqrt{2} \in K$ (mais en fait cet invariant est toujours 0 !)

Principe basé sur le théorème de Springer.

On peut supposer que $\varphi(G_K) \subset S_2(A_6)$

(141)

$\varphi_E(G_K) \subset S_2(A_6) = D_4$



$D_4 \subset S_4$, $D_4 \subset S_2$, combined
pour sign. 1.

On peut calculer la forme quadratique
grâce à ça.

Question finale : $n=6$

S_6 a un automorphisme extérieur

$$\text{Out}(S_6) = \mathbb{Z}/2\mathbb{Z}$$

(alors que $\text{Out}(S_n) = \{1\}$ pour $n \neq 6$)

$\sigma \in \text{Out}(S_6)$, non dans S_6

E algèbre étale, $\varphi: G_K \rightarrow S_6$

$$\downarrow \sigma$$

$$\sigma \varphi_E = \varphi_{E'}$$

algèbre étale

"Résolvante sextique" d'un polynôme
de degré 6

$f_6 \mapsto f_6'$ tel que, généralement, 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 $O^+(S_6)$

$$\text{et } \varepsilon_6^2 \mapsto \varepsilon_6^2$$

$$s_6 \mapsto s_6 + \varepsilon_6^2$$

$$(12) \mapsto (12)(34)(56).$$

Supposons $(d) = (1)$, $\varphi_E(G_K) \subset A_6$.

Théorème :
$$\boxed{q_E' \cong 2q_E}.$$

On peut donner des exemples où $q_E' \neq q_E$, 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 $\varphi_E(G_K) \subset S_2(A_6) = D_4$.

$$E = K_4 \times K_2$$

$$D_4 \quad D_2$$

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 $G \xrightarrow{\rho} A_7$
 $\xrightarrow{\rho'} A_7$
 $\text{Aut}((2,2,2))$

action sur 7 points $\rightarrow \rho$ et ρ' .
 et droites

D'où

$$\begin{array}{ccc} \varphi: G_K & \rightarrow & G \\ & & \swarrow \quad \searrow \\ & & A_7 \end{array}$$

d'où 2 algèbres ~~galoisiennes~~ étale
 de rang 7, E et \widehat{E} .

Facile à voir que q_E et $\widehat{q_E}$ ont
 le même $w_1 (=0)$

- " -

w_2

Théorème :

On a

$$q_E \cong \langle 1 \rangle \oplus \varphi_6$$

144

$$q_E \cong \langle 1 \rangle \oplus 2 \varphi_6$$

On φ_6 est de rang 6

On a : $q_E \cong \langle 1 \rangle \oplus \underbrace{\langle 1 \rangle \oplus \langle 2 \rangle}_{\varphi_6} \oplus \langle 2 \rangle \oplus \varphi_4$

Ceci découle du thm sur A_6 .

Par Springer, on peut supposer que

$$\varphi(G_K) \subset S_2(G) = D_4$$

$$D_4 \hookrightarrow A_6 \hookrightarrow A_7 \quad \text{bien à l'}$$

$\downarrow \begin{smallmatrix} \alpha^{-1} \\ \text{ext} \\ A_6 \end{smallmatrix}$

$$D_4 \rightarrow A_6 \rightarrow A_5 \rightarrow A_7$$

$\downarrow \begin{smallmatrix} \text{ext} \\ \alpha^{-1} \end{smallmatrix}$

$$E = K \times E_6 \quad , \quad E' = K \times E'_6$$

$$q_E = \langle 1 \rangle \oplus q_{E_6}$$

$$q_{E'} = \langle 1 \rangle \oplus q_{E'_6}$$

$$\Rightarrow q_{E'_6} \cong 2 q_{E_6}$$

Retour sur l'exemple quintique:

$|K|=9$ les coins sont en fait trois disjoints corps $\mathbb{F}_3, \mathbb{F}_7, \mathbb{F}_9$. L'algèbre étale de \mathbb{F}_5 sur K d'ind 5 (mod 5) est de la forme $K[x]/x^5 + a_1x^4 + \dots + a_5$ avec $a_1 = a_2 = 0$.

classe de conjugaison $c \in S_5$

Quand 5 est un carré ($q=9$), c doit être de A_5

pas ($q=3 \text{ ou } 7$), c — de $S_5 - A_5$

de A_5 $c = (1), (12)(34), (123), (12345)$

de $S_5 - A_5$ $c = (12), (123)(45), (1234)$

$$E = \underbrace{\mathbb{F}_q \times \dots \times \mathbb{F}_q}_{5 \text{ fois}}, \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \mathbb{F}_q, \mathbb{F}_{q^3} \times \mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q$$

$$\text{et resp } E = \mathbb{F}_{q^2} \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_{q^3} \times \mathbb{F}_{q^2}, \mathbb{F}_{q^4} \times \mathbb{F}_q.$$

On est amené à trouver les polynômes correspondants

Exemple $q=3$

$$F = \underbrace{(x^3 - x)}_{\substack{\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \\ (3 \text{ racines})}} \underbrace{(x^2 + 1)}_{\mathbb{F}_{q^2}} = x^5 - x$$

$$f = \underbrace{(x^3 - x + 1)}_{\substack{\text{irred de} \\ d^0 3}} \underbrace{(x^2 + 1)}_{\mathbb{F}_{q^2}} = x^5 + x^2 - x + 1$$

$$f = \underbrace{(x^4 + x - 1)}_{\substack{\text{irred de } d^0 4}} x$$

Algèbres à involution

146

K car $K \neq \mathbb{Z}$

A K -algèbre associative, élémt unité, de dimension finie³¹ munie d'un anti-automorphisme involutif $x \mapsto x^*$ (ou x^1, x^2, \dots)

$\begin{cases} x \mapsto x^* \text{ est } K\text{-linéaire} \\ (xy)^* = y^* x^* \\ (x^*)^* = x \end{cases}$

Structure $r =$ radical de A

r est stable par $x \mapsto x^*$

$$0 \rightarrow r \rightarrow A \rightarrow B \rightarrow 0$$

$B = A/r$ 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.

$$C = \prod_{\beta \text{ fixe}} K_\beta \times \prod_{\substack{\gamma \text{ et } \gamma' \\ \text{échogés}}} (K_\gamma \times K_{\gamma'})$$

L'algèbre B est aussi découpée en

$$B = \prod_{\alpha} B_\alpha \times \prod_{\gamma} B_\gamma$$

Yens
de repres.
": $\gamma^* + \gamma$ ".

centre de B_α est K_α un corps, B_α simple
centre de B_γ est $K_\gamma \times K_\gamma$ (échogés 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_β et $K_{\beta'}$,
 sur K_β : action tri-nale ou par K_β/K_β^0 quadratique.

Hypothèse provisoire K alg^{cl}

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 se échangent par l'involution

①

$x \mapsto x^*$ anti-automorphisme

Or $x \mapsto {}^t x$ est involution

On sait que les automorphismes se intègrent $x \mapsto yxy^{-1}$

Donc il existe $y \in A^{\times}$, tq

$$x^* = y {}^t x y^{-1}$$

$$x^{**} = y(y {}^t x y^{-1}) {}^t y^{-1} = y {}^t y^{-1} x {}^t y y^{-1}$$

$$\text{donc } {}^t y y^{-1} = 1 \in K^\times \quad {}^t y = \pm y \text{ donc } 1 = \pm 1$$

d'où 2 possibilités $1 = 1$, $y = {}^t y$ cas orthogonal

$\} 1 = -1$, $y = -{}^t y$ cas symplechi.

Ceci n'est possible que si n pair

② Si on identifie le 1^e morceau^{ops} le second tel que $(x, y) \mapsto ({}^r y, {}^t x)$.

K non alg. clos

(148)

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 involut. orthog ou sympl.

② L non fixé

Le ~~non~~ corps fixé

$A \otimes_{L_0} L_s$ est du 2^e type

③ $L \times L$

$A \simeq B \times B^o$ B alg. simple centrale
les deux facteurs étant échangés par
l'involution

cas séparable 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 .

m impair Toute similitude est produit
d'un scolave et d'une tr. orth.

m pair 2 hypers $\langle x, y \rangle = 2 \langle x, y \rangle$
 $m = 2m$ dét (s) $= \pm 2^m$

type similitude \rightarrow $\begin{cases} n \text{ impair} & \text{Aut} = O_n / \{I\} = SO_n \\ n \text{ pair} & \text{Aut}^0 \text{ indice 2 dans Aut} \\ & \text{Aut}^0 = O_n / \{I\} \end{cases}$ (149)

type symplect. \rightarrow $\begin{cases} \text{Aut}^0 \text{ indice 2} & \text{Aut}^0 = O_n / \{I\} \\ \text{Aut}^0 = PGL_n & \text{Aut}^0 = Sp_n / \{I\} \end{cases}$

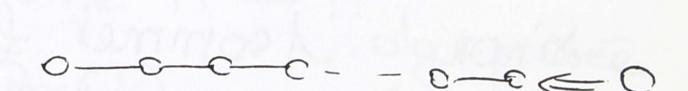
Comparaison aux diagrammes de Dynkin (des groupes classiques)

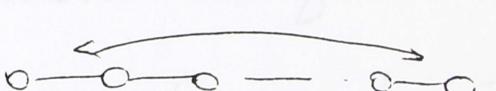
type 1 n impair $B_{\frac{n-1}{2}}$ 
 $n \neq 1$ pas d'autom. externes.
c'est complète.

n pair $D_{\frac{n}{2}}$ 

type sympl.

type 2 compos.

$n \neq 1, 2$ $C_{n/2}$ 

A_{n-1} 

K A algèbre déployée simple.
(comme algèbre associative).

cas orthogonal : forme standard = $\begin{cases} \text{hyperbol. si } n \text{ pair} \\ (\text{1}) \text{ hyperb si } n \text{ impair} \end{cases}$

$A \rightarrow$ gpe simple (adjt) = comp neutre
/ ole Aut A
G déployé.
de l'un des types
classiques.

(150)

On a aussi un isomorphisme de $\text{Aut } A \rightarrow \text{Aut } G$.
 [Weil, OC, II] les K -formes de A correspondent aux K -formes de G .

A l'exception des formes de D_4 "trialitaires"
toute K -forme d'un groupe classique (simple abs)
s'obtient à partir d'une alg. à involution
 ("simple de centre K ")

Action de G_K sur le schéma :

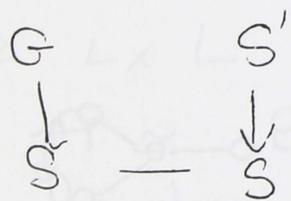
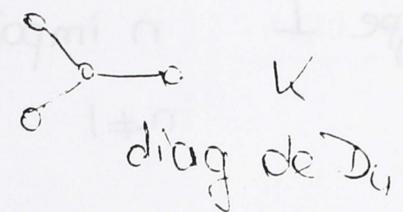


schéma des schémas de Dynkin



trialitaire : les 3 sommets est. et permutes.
 minor 1 sommet fixe 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 $\text{Cor}_{L/K} [A]_L = 0$ ds $\text{Br}(K)$.

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 $\text{Cor}_{L/K} [A]_L = 0$ ds $\text{Br}(K)$.

Démonstration du 1^{er} théorème

* définit un isomorphisme $A \rightarrow A^\circ$
donc $[A] = [A^\circ]$ ds $\text{Br}(K)$ alg opposée
= $-[A]$.

Réiproquement, ^{l'opposé 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 $(d_{ij}) \rightarrow (d_{ji}^*)$

Soit L un corps commutatif maximal de A $[A : K] = n^2 \Rightarrow [L : K] = n$

lemme (a) Il existe un anti-isomorphisme $A \rightarrow A$ qui est l'identité sur L .

(b) Un tel anti-isomorphisme est une involution.

(a) Choisissons un anti-isomorphisme $i: A \rightarrow i(A)$ de A .
 $i_L = \text{rest. de } i \text{ à } L$ est un isomorphisme de L sur $i(L)$.

Donc il existe (Skolem-Noether) $a \in A^\times$ tel que $i(x) = axa^{-1}$ pour tout $x \in L$.

L'anti-isomorphisme $x \mapsto a^{-1}i(x)a$ possède la propriété voulue en a).

(b) est un énoncé géométrique: il se vérifie par ex. des scolaires. Alors A devient $M_n(K)$ et L devient l'algèbre diagonale $Kx^{-1}xK \hookrightarrow M_n(K)$.

Soit i un anti-isomorphisme $A \rightarrow A$.

Il existe $a \in A^\times$ tq $i(x) = a^+ x a^{-1}$.
 $a^+ x a^{-1} = x \quad x \in L$

$\Rightarrow a$ commute à L

$\Rightarrow a \in L^\times \quad a = \begin{pmatrix} \mathbb{I} & 0 \\ 0 & \mathbb{I} \end{pmatrix}$

d'où $i^2(x) = a(\mathbb{I} a^{-1} x \mathbb{I} a) a^{-1} = x$.

Si $[A] = [A^\circ] \Rightarrow$ involution existe | de type \perp (négatif)
 de type alterné (négatif)

La méthode donne \perp par construction.

Pour le type alterné, il P s'en déduit:

on * type \perp ,

on choisit $a \in A^\times$ avec $a^* = -a$. (existe si n pair)

$x^\perp = a x^* a^{-1}$ définit une involution de type symplectique.

Reste à clouser $a \in A^*$ $a^* = -a$

$a \in A^*$: donne un ouvert de Zariski de A .

Supposons K infini

Sur A , l'ensemble des éléments anti-invariants par $*$. On doit voir que A ne 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 existent des formes alt non dégénérées si n pair.

Remarque: A irr. simple de centre K $rg = m^2$
 $A_+ = \{a, a^* = a\}$ $\dim A_+ = \frac{m(m+1)}{2}$
 dans le cas orthogonal

$$= \frac{m(m-1)}{2}$$

dans le cas symplectique

2^e thme: preuve

A centrale simple sur L , L/K quadratique
 K -involutions de 2^e espèce, non triviales sur L

A sur L

$\lambda \mapsto \bar{\lambda}$ invol de L

$\mathcal{O}\bar{A}$ algèbre réduite de A par changement de base $L \xrightarrow{\lambda \mapsto \bar{\lambda}} L$.

⑨ A vue comme L -algèbre par $L \xrightarrow{\cdot} L \xrightarrow{\cdot} A$. (154)

⑩ $\bar{a} \in \bar{A}$

$$(\bar{ab}) = \bar{a} \bar{b}$$

$$\bar{\bar{a}} = \bar{\bar{a}} \quad \lambda \in L$$

Une involution de 2^e espèce définit un anti-isomorphisme $A \xrightarrow{\cdot} \bar{A}$, i.e. $A^0 \simeq \bar{A}$.

où condition nécessaire et suffisante

$$[A^0] = [\bar{A}] \text{ ds pr (1)}$$

$$\text{i.e. } [A] + [\bar{A}] = 0. \quad (+)$$

Soit A satisfaisant à $[A] + [\bar{A}] = 0$.

Il existe $i: A \xrightarrow{\cdot} A$ tq $i(x, y) = i(y) \bar{i}(x)$
 $i(\lambda) = \bar{\lambda} \quad \lambda \in L$.

$\left\{ \begin{array}{l} i: \text{anti-linéaire} \\ \text{anti-isomorphisme} \end{array} \right.$

Si i est comme ci-dessus,

$x \mapsto i^2(x)$ L -automorphisme de A .

Il existe $a \in A^\times$ tq $i^2(x) = a x a^{-1} \quad \forall x \in A$

$$\begin{aligned} i^3(x) &= i(i^2(x)) = i(a^{-1}) i(x) i(a) \\ &= i^2(i(x)) = a i(x) a^{-1}. \end{aligned}$$

$$\Rightarrow \text{Il existe } \lambda \in L^\times \quad \lambda = a i(a) \\ = i(a) a$$

$$i(\lambda) = i^2(a) i(a) = a i(a) = \lambda$$

donc $\lambda \in K^\times$.

Que donnent d'autres choix?

$a \mapsto \mu a \quad \mu \in L^{\times}$ λ défini à NL^{\times} près.

On peut aussi changer de i , mais en fait:

λ vu comme élé de K^{\times} / NL^{\times} ne dépend ni du chx de a , ni de celle de i .

$i'(x) = b_i(x) b_i^{-1}$ et calcul. (cf Scharlau)

$K^{\times} / NL^{\times} = \text{Br}(L/K) = \text{Ker: Br } K \rightarrow \text{Br } L$.

lemme. L'élément $(\lambda) \in \text{Br}(L/K)$ est le cor $\text{Cor}_{L/K}^{\lambda}$

Si une invol existe, on a $\lambda = 1 \Rightarrow \text{Cor} = 0$

Invers si $\text{Cor} = 0$, $\lambda = \mu \bar{\mu}$

on chge pr que $\lambda = 1$, $a i(a) = 1$.

on chge de i !

$i \mapsto b_i b_i^{-1} \quad \lambda(x) = b_i(x) b_i^{-1}$

$\lambda^2(x) =$

(voir p. 158, Correction) $= b_i(b_i^{-1}) a x \bar{a}^{-1} i(b) b_i^{-1}$

d'où $b_i(b_i^{-1}) = \bar{a}^{-1}$ ie $a \in \text{Im}(i^{-1})$. ok

Preuve du lemme B alg sur L (quad / K)

$\text{Vect}_L \longrightarrow \text{Vect}_{L/K}$

$V \otimes \bar{V}$ $\text{Gal}(L/K)$ 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

$$W = \text{Cor}_{L/K} V$$

Se définit plus généralement dès que L/K séparable et descendante à Weil.

On devrait appeler cela $N_{L/K} V$ "norme" de V .

[Par contre $\text{Tr}_{L/K} V = V$ vu comme K -esp. vectoriel obtenu par descente à partir de la somme directe des conjugués -]

$$\text{On a } N(V \otimes V') = N(V) \otimes N(V').$$

B alg sur $L \rightarrow \text{Cor}_B =$ K -alg. de $B \otimes \bar{B}$ formée des invariants de $\sum \bar{Q}_i \otimes \bar{C}_j \mapsto \sum C_j \otimes \bar{C}_j$ (cf Riehm, Inv.).

$$A \otimes_L \bar{A} = \Delta \otimes_K \bar{\Delta} \quad \Delta = \text{Cor}_\mathbb{Q} A$$

algèbre centrale simple sur K

H alg. de quaternions définie par $(L/K, \Delta)$

$$H = L \oplus L \cdot \varphi$$

$$\varphi^2 = 1$$

$$\varphi \ell \varphi^{-1} = \ell \text{ pour tout } \ell \in$$

On va voir que $\Delta \otimes_K H$ est isomorphe à une alg. de matrices, d'où $[\Delta] + [H] = 0 \Rightarrow [\Delta] = 0$

$$\text{On a: } \dim_K \Delta = n^2$$

$$\dim_K H = 4$$

$$\dim_K \bar{A} = 2n$$

On définit deux plongements

$$\Delta \rightarrow \text{End}_K A (\simeq M_{2n}(K))$$

$$H \rightarrow \text{End}_K A$$

de sorte que les images soient le commutant
l'une de l'autre d'où isomorphisme voulu

$$\Delta \underset{K}{\otimes} H \simeq \text{End}_K A.$$

(car les dimensions sont bonnes).

$$\Delta \subset A \otimes \bar{A}$$

$$A \underset{L}{\otimes} \bar{A} \rightarrow \text{End}_K A$$

$$x \otimes \bar{y} \mapsto u_{x, \bar{y}}(z) = xz\bar{i}(y) \quad z \in A$$

$$H = L \oplus L\varphi \quad \varphi^2 = \lambda$$

$$L \rightarrow \text{End}_K A$$

$$\varphi \mapsto \underline{\varphi} \in \text{End}_K A \quad \underline{\varphi}(z) = i(z)a \quad z \in A$$

$$\text{Vérifions: } \underline{\varphi^2}(z) = i(i(z)a)a = i(a)i^2(z)a = \dots = i(a)aza^{-1}a = \lambda z.$$

On a de plus $u_{x, \bar{y}} \circ \varphi = \varphi \circ u_{y, \bar{x}}$, d'où le fait que les images de Δ et de H dans $\text{End}_K(A)$ commutent. D'où le résultat cherché.

1) Corrections: 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~~ 19762)
et peut être marche dès que

$$\begin{cases} A_S \\ \mathbb{P}_1 \end{cases}$$

2) A de 2^e espèce $a^* = 1 \Rightarrow a \stackrel{?}{=} b' b^*$

① On pourrait supposer que A est un corps (gau de Cor = 0).

② Si $a = -1 \Rightarrow i^2(a) = a^* a^{-1} = x$, i involution

③ Si $1+a$ est inversible et $b = \frac{1}{1+a}$ connu

$$b^* = \frac{1}{1+a^{-1}} = \frac{a}{1+a} \quad b^{-1} b^* = a$$

A est une k -algèbre à involution $*$, car $k \neq 2$

éléments hermitiens (ou symétriques) $a^* = a$: H_A

antihermitiens A_-

$$A = A_- \oplus H_A$$

unitaires U_A : $a^* a = 1$.

On souligne les lettres pour indiquer les variétés algébriques correspondantes

$$H_A(k) = H_A$$

$$H_{A_-}(k') = H_{A \otimes_k k'}$$

$U_A \subset GL_A$ (groupe multiplicatif de A)

159

$$GL_A(K') = (A \otimes_{K'} K')^\times$$

hermitiens inversibles

$$H_A^\times$$

Th:

$$GL_A / U_A \simeq H_A^\times$$

(comme variétés algébriques)

$x \in GL_A$ $h \in H_A$ $x h x^* \in H_A$ d'où une action de GL_A sur H_A^\times (en particulier H_A^\times).

L'action sur H_A^\times est transitive et le stabilisateur

de $h = 1$ est U_A .

montrer:

$$GL_A \longrightarrow H_A^\times \text{ lisse}$$

$$x \mapsto x \cdot 1 \cdot x^* = xx^*$$

L'application tangente à l'origine :

$$x = h \varepsilon$$

$$\begin{cases} \varepsilon^2 = 0 \\ \varepsilon \varepsilon^* = 0 \end{cases}$$

$$h \mapsto H_A$$

$$\varepsilon \mapsto \varepsilon + \varepsilon^*$$

surjective

$$(h + \varepsilon)(1 + \varepsilon^*) = \dots$$

$$\text{car: } \varepsilon + \varepsilon^* = \eta \quad \varepsilon = \frac{1}{2}\eta \text{ marche}$$

Plus généralement:

$$GL_A \longrightarrow H_A^\times$$

$$x \mapsto x h x^* \quad h \in H_A$$

L'appl. tgte est $\varepsilon \mapsto \varepsilon h + h \varepsilon^*$, est aussi surjective

[Si $\eta \in H_A$ on pose $\varepsilon = \frac{1}{2}\eta h^{-1}$, et l'on a:

$$h \varepsilon + h \varepsilon^* = \frac{1}{2}\eta + \frac{1}{2}h(h^{-1}\eta^*)$$

$$= \frac{1}{2}\eta + \frac{1}{2}\eta = \eta \cdot]$$

d'appl. togé est sujective, les orbites sont ouvertes

H_A^X ouvert d'un ev., irreductible, connexe donc il y a une seule orbite. Donc le résutat inversible

Tout élé. hermitien V est donc du type $\mathfrak{so} \mathfrak{so}^*$ après extension des scalaires.

Ce point se démontre en fait directement: si K alg. clos, tout hermitien $^{\text{inv.}}$ est le carré d'un hermitien. En effet

lemme Si K alg. clos de car $\neq 2$ et si E est une alg. de dim finie sur K , H él. inversible de E est un carré.

(On applique où $E = \text{alg. eng. par un él. hermitien}$

$$1 \rightarrow \underline{U}_A \rightarrow \text{GL}_A \rightarrow H_A^X \rightarrow 1$$

espace homogène

$$A^X \xrightarrow{\quad} H^0(K, H_A^X) \xrightarrow{\quad} H^1(K, \underline{U}_A) \xrightarrow{\quad} H^1(K, \text{GL}_A)$$

" " " thme 90".

H_A^X

cf LN 5 Interprétation de la suite exacte:

$$\left[H^1(K, \underline{U}_A) \simeq H_A^X / \text{action de } A^X \right]$$

action de A^X : $a \in A^X \mapsto aRa^*$

classes de
modules hermitiens $\simeq \mathcal{H}(K, U_A)$
de rang 1 non
dégénérées

161

M A -module à gauche (de type fini)
 A forme hermitienne sur M

$$h: M \times M \rightarrow A$$

$$h(am_1, m_2) = a h(m_1, m_2)$$

$$h(m_1, am_2) = h(m_1, m_2) a^*$$

$$h(m_1, m_2) = h(m_2, m_1)^*$$

$$a \in A \quad m_i \in M$$

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 dans le cas de dim finie!).

Cas particulier M libre de rang 1. $M = Ae$
 $h(e, e)$ suffit pour tout connaitre

$$h = h(e, e) \in H_A^x$$

Choix de base le transforme en $a h a^*$

Aut A "voisin" du groupe des automorphismes des groupes simples classiques.

$$U_A \longrightarrow \text{Aut } A$$

$x \in U_A \quad x \mapsto uxu^*$ 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 $\text{Aut } A$ 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

$$H^1(K, U_A) \longrightarrow \prod_v H^1(K_v, U_A)$$

n'est pas toujours injective

Exercice: A algèbre de quaternions sur K

$*$ = involution de A différente de l'involution standard.

$$\dim U_A = 1$$

2 comp. connexes

celle de l'elt neutre est un tore

[Soit $a \in A^\times$ avec $\bar{a} = -a$ (" $-$ " = invol. stand.)]

$$\text{On pose: } x^* = a \bar{x} a^{-1}$$

Par un choix convenable de l'involution (bcp de places ramifiées, au moins 4 marche).

principe de Hesse faux ("c'est le seul cas"). (163)

② Invariants de tenseurs quadratiques

V esp. vect. de dim finie sur K

Soient v_1 des "tenseurs quadratiques" i.e. des éléments de $\otimes^2 V$, $V \otimes V'$, $\otimes^2 V'$.

Soit G_v le fixateur de ces éléments GL_V

Alors G_v est isomorphe au groupe

Unitaire U_A d'une algèbre à invol. canon.

Car intersection de gpos orthog (et symplectiques) est un gpe unitaire.

Remarque: cubique ne marche pas

- G_8 rep. mixte $d^0 7$
forme trilinéaire alternée $\rightarrow G_2 \times F_4$
- E_6 est aussi possible (rep. de $d^0 27$).

Application par Eva à pr. de principe Hesse faux.

Preuve de ②:

On va construire une alg. à involut A

$$A \subset \text{End}(V) \times \text{End}(V') = R \quad V' = \text{dual}$$
$$(f, g) \mapsto ({}^t g, {}^t f)$$

Pour tout tenseur v quadratique, on va définir $A_v \subset R$

$$③ v \in V \otimes V' = \text{End}(V)$$

$$V \xrightarrow{v} V$$

$A_v = \{ (f, g) \text{, avec } fv = vf \text{, et } {}^t g v = v^t g \}$.

(f, g)

fixateur de v est égal à U_{A_v}

ici $\begin{array}{l} fv f^{-1} = v \\ fv = vf \end{array}$

$f v = v f$

$U_R = \{ (f, {}^t f^{-1}) \} \quad f \in G(V)$

b) $v \in V \otimes V$

$\begin{array}{c} \parallel \\ \text{Hom}(V, V') \end{array}$

$V \xrightarrow{v} V'$

$$\begin{array}{ccc} f \downarrow & f, g & A_v = \{ (f, g) \mid gv = vf \} \\ V \xrightarrow{v} V' & & {}^t fv = v^t g \end{array}$$

On vérifie que ceci définit algébriquement et que le fixateur est le gpe unitaire grâce aux "2 cond" ne dépend pas de la manière de voir v comme hom.

① $v \in V' \otimes V'$ m chose.

ou encore v interprété comme forme bilinéaire

$B_v: V \times V \rightarrow K$

$$(f, g) \in R_v \iff \begin{cases} B_v(fx, y) = B_v(x, {}^t g y) \\ B_v(gx, y) = B_v(x, {}^t f y) \end{cases}$$

Problème

Existe-t-il un plongement de G_2 dans un groupe semi-simple G et des sous-groupes H_2 de G isomorphes orth. (ou sympl.) tels que $G_2 = \cap H_2$?

(En particul. on ne demande plus flgt général ds un GL avec l'ident nulle).
en g.al : on plonge ds Λ quadratiques.

Théorème (Bayer-Lenstra) Soit A une algèbre à invol. Soit K'/K une ext de d^0 impair
Alors $H^1(K, U_A) \rightarrow H^1(K', U_A)$ est injective.

Plusieurs réductions:

→ radical

$\Gamma_A \subset A$ $\begin{cases} A/\Gamma_A \text{ semi-simple} \\ \Gamma_A \text{ idéal nilpotent} \end{cases}$

Th : $H^1(K, U_A) \rightarrow H^1(K, U_{A/\Gamma})$ est bijective

Par ex : en interprétant avec les hermitiens (inversible \Leftrightarrow image mod rad. inv.).

Ou encore $1 \rightarrow N \rightarrow U_A \rightarrow U_{A/\Gamma} \rightarrow 1$,
 $N = \text{unipotent déployé} = \text{ext. succ. de } \mathbb{G}_a$
donc à colom. finie.

On peut supposer $K' = K(x)$ monoïgène

On choisit un tel x , d'où une forme linéaire $\lambda : K' \rightarrow K$, $\lambda(1) = 1$ et $\lambda(x^i) = 0$, $1 \leq i \leq m-1$

M_1 et M_2 modules hermitiens sur A non dégénérée libre de rang 1.

$$K' \otimes_{\mathbb{K}} M_1 \simeq K' \otimes_{\mathbb{K}} M_2 \Rightarrow M_1 \simeq M_2$$

Si M' est un A' -module hermitien de

rang 1, on définit $\lambda(M')$, A -module hermitien de rang $n = [K : K]$ par :

$$\lambda(M') = M' \text{ comme } A\text{-module}$$

$$\begin{array}{ccc} M' \times M' & \rightarrow & A \\ \searrow & \nearrow \lambda \otimes 1 & \\ A & & K' \otimes A \end{array}$$

$$\underline{M'}_1 = K' \otimes M_1$$

↓

$$N_1 = \lambda(M'_1) \text{ de rang } n \text{ sur } A.$$

On peut donner la structure de ce module

K' esp. quad. sur K

$$(x, y) \mapsto \lambda(xy)$$

$$K' \simeq \langle 1, 1, -1, 1, -1, -1, 1, -1 \rangle$$

$$\simeq \langle 1 \rangle + \mathfrak{h}$$

hyperbolique

$$K' = K_1 \oplus H' \oplus H''$$

↑ ↑
totale isot

$$N_1 \simeq M_1 \oplus \underbrace{H'_1 \oplus H''_1}_{\text{totale isotropes}}$$

libres de rg $\frac{m-1}{2}$

idem pour N_2

$$H'_1 \oplus H''_1 \simeq H'_2 \oplus H''_2$$

Thème de simplification de Witt est vrai du cas
hermitien (cf exposé d'Eva ci-après)

$$\text{d'où } M_1 \simeq M_2$$

Thme de Witt Hermition

Fin de la réduction

$$H^1(K, U_A) \rightarrow H^1(K', U_A) \quad \text{injective}$$

K'/K d'impair

On peut supposer que A est semi-simple, en fait m algèbre à involution simple:

$$A = A_1 \times \cdots \times A_r \times A_{r+1} \times A_{r+1}^* \times \cdots \times A_g \times A_g^*$$

Certaines sont invariantes par involution. $A_i = A_i^*$
D'autres échangées.

$$H^1(K, U_A) = H^1(K, A_1) \times \cdots \times H^1(K, U_{A_r})$$

$$\times H^1(K, U_{A_{r+1} \times A_{r+1}^*}) \times \cdots \times H^1(K, \underbrace{A_{r+1} \times U_{A_{r+1} \times A_{r+1}^*}}_{\text{D}})$$

$$\times \underbrace{H^1(K, U_{A_g \times A_g^*})}_{\text{D}}$$

$$U_{B \times B^*} = G_B \quad \text{et "Hilbert 90".}$$

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 .

$$= Ax \oplus A y \quad \text{muni } \langle x, x \rangle = \langle y, y \rangle = 0.$$

de $\langle x, y \rangle = 1$

Alors $N_1 \cong N_2$

Reques: $\langle , \rangle = f$ ds la notation antérieure
On suppose t's les mod hermitiens non dégénérés (vrai si c'est au

On appelle (x, y) paire hyperbolique

Remarque: 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 $N \oplus M \cong A^m$

$$\text{d'où } (N_1 \oplus H(A))^m \cong N_2 \oplus H(A)^n$$

et par récurrence se déduit du thm énoncé.

Ref: B. Keller Not. Zeit. 1988.

M. Knus livre à paraître chez Springer.

(Quettbemann, R. Scharlau, W. Scharlau, Schulte,
Mémoires SMF ~ 1976 très général).

Démonstration

$M = N \oplus H(A)$ forme hermitienne \langle , \rangle

(x, y) paire hyperbolique

Lemma $U(M)$ agit transitivement sur
l'ensemble des plans hyperboliques
de M .

Lemma \Rightarrow théorème

$$M = N_1 \oplus H_1 = N_2 \oplus H_2$$

$$\varphi: M \rightarrow M \quad \varphi(H_1) = H_2, \text{ alors } \varphi(H_1^\perp) = H_2^\perp$$

$$\begin{matrix} & & \\ \parallel & & \parallel \\ N_1 & & N_2 \end{matrix}$$

Transvections $(M, < >)$

170

Soient $u \in M$ $\langle u, u \rangle = 0$.

$v \in M$ $\langle u, v \rangle = 0$.

$a \in A$ tel que $a + \bar{a} = \langle v, v \rangle$.

Posons: $\sigma_{u, a, v}(x) = xc + \langle x, v \rangle u - \langle x, u \rangle v - \langle x, u \rangle a$

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) $\sigma_{u, a^1, v^1} \circ \sigma_{u, a, v} = \sigma_{u, a+a^1+v^1, v}$

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

$\alpha \in A^*$ $H_{x, y}(\alpha) \in U(H) \subset U(M)$

$$H_{x, y}(\alpha)(x) = \alpha x$$

$$H_{x, y}(\alpha)(y) = \bar{\alpha}^{-1} y$$

On note $G(M, x, y)$ le sous-groupe de $U(M)$ engendré par les transvections $\sigma_{u, a, v}$ avec $u \in Ax \cup Ay$ $v \in N$ et par les $H_{x, y}(\alpha)$, $\alpha \in A^*$.

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:

$$x' = \alpha x + \beta y + u \quad u \in N$$

Si $\alpha \in A^\times$ alors il existe $\varphi \in G(\pi, x, y)$ tq
 $\varphi(x) = x'$ et $\varphi(y) = y'$.

Démonstration

$$0 = \langle x', x' \rangle = \alpha \bar{\beta} + \beta \bar{\alpha} + \langle u, u \rangle$$

$$\text{d'où } \langle u, u \rangle = -\alpha \bar{\beta} - \beta \bar{\alpha}.$$

$$\langle \alpha^{-1}u, \alpha^{-1}u \rangle = -\bar{\beta} \bar{\alpha}^{-1} - \bar{\alpha}^{-1} \beta$$

$$\sigma_y, -\alpha^{-1}\beta, -\alpha^{-1}u \in G(M, x, y)$$

$$\sigma_y, -\alpha^{-1}\beta, -\alpha^{-1}u (x) = \alpha^{-1}x'$$

$$\gamma = H_{x, y}(\alpha) \circ \sigma_y, -\alpha^{-1}\beta, -\alpha^{-1}u$$

$$\gamma^{-1}(y') = \gamma x + \delta y + v$$

$$\langle \gamma^{-1}(x), \gamma^{-1}(y') \rangle = 1 = \langle x, \gamma x + \delta y + v \rangle = \delta$$

$$\langle v, v \rangle = -\gamma - \bar{\gamma}$$

$$\sigma_{x, -\gamma, -v}(x) = x$$

$$\sigma_{x, -\gamma, -v}(y) = \gamma^{-1}(y').$$

Posons

$$\varphi = \psi \circ \sigma_{x, -\beta, -v}$$

$$\text{On a : } \varphi(x) = x'$$

$$\varphi(y) = y'.$$

Remarque. Soit $z \in N$, $\langle z, z \rangle = p + \bar{p}$

$$\sigma_{x, p, z}(x') = (\alpha - \beta p + \langle u, z \rangle)x + \dots$$

Donc il suffit de trouver un z dans N

$$\begin{cases} (\alpha - \beta p + \langle u, z \rangle) \text{ soit inversible.} \\ \langle z, z \rangle = p + \bar{p} \end{cases}$$

• Corps gauches $A = \mathbb{D}$.

Soit (x', y') une "autre paire".

$$x' = \alpha x + \beta y + u$$

Si $\alpha \neq 0$ OK.

Sinon il faut trouver $z \in N$ $\langle u, z \rangle = \beta p \neq 0$.

Si $u \neq 0$ on peut trouver $z \in N$ tq $\langle u, z \rangle$ soit une paire hyperbolique

Si $u = 0$ OK aussi avec $z \neq 0$.

Soit M un module hermitien, $M \in H(A)^n$.

Soient $(x_1, y_1), \dots, (x_n, y_n)$ 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 m -uples de paires hyperboliques

Orthogonaux deux à deux.

173

Démonstr. par récurrence

Algèbres simples

Soit \mathbb{D} un corps gauché muni d'une involution $\mathbb{D} \rightarrow \mathbb{D}$

$A = M_n(\mathbb{D})$ et soit $*: A \rightarrow A$ involution donnée par $(d_{ij})^* = (\bar{d}_{ji})$.

Soient $e_{ij} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$

$e_{11} = e$ 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 $\mathbb{D} = eAe$

2) eH est la somme \perp de n plans hyperboliques $H_i \cong H(\mathbb{D})$ avec paire hyperbolique $(e_{1i}x, e_{1i}y)$.

3) Tout élément de $U(eM)$ s'étend de façon unique en un élément de $U(M)$.

Reve: $e = e_{11}$ est bien un projecteur hermitien.

Theorème

174

- 1) $G(eM, e_1, x, e_1, y) \subset G(M, x, y)$
- 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 plan hyperbolique engendré par $e_1 x, e_1 y$
 $z = e_1 x$ ou $e_1 y$ ou multiple et $u \in H^+$.

Si $u \in H^+ = N \quad \sigma_{z, a, u} \in G(M, x, y)$

Si non soit $u = v + w$ avec $v \in H$
 $w \in H^+ = N$

$$\sigma_{z, a, u} = \sigma_{z, b, v} \circ \sigma_{z, c, w} \quad \begin{cases} b + b^* = < v \\ c + c^* = < w \end{cases}$$

$\sigma_{z, c, w} \in G(M, x, y)$

$$\sigma_{z, b, v}(x) = \alpha' x + \beta' y \quad \text{On voit que } \alpha' \in \mathbb{A}^*$$

Il existe par la proportionnalité du debut une

$$\varphi \in G(H, x, y) \quad \text{avec } \varphi(x) = x' \quad \varphi(y) = y' \\ \text{donc } \varphi = \sigma_{z, b, v}$$

Reste le cas où l'involution \sim est quelconque.
Il existe une unité $c \in A^*$ telle que
 $\tilde{x} = cx^* c^{-1}$

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^*y) est une paire hyperbolique pour $(M, <, >_c)$.

3) Les sous-groupes du groupe unitaire se correspondent.

$$G(M, <, >, x, y) = G(M, <, >_c, x, c^*y).$$

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 $q: V \rightarrow K$ 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
galochienne sur K

Exemple 2 V base $(e_g)_{g \in G}$,
 $g \cdot h = e_{gh}$ (\bar{a} 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

$g \cdot e$ ($g \in G$) base de V

$$q(e, g \cdot e) = 0 \quad \text{si } g \neq 1 \\ = 1 \quad \text{si } g = 1$$

L/K a une base normale auto-duale (BNA)

"belle base"

Si: $(L, q_L, \text{action de } G) \simeq G$ - forme quadratique unité

\Leftrightarrow il existe $e \in L$, tel que:

(ge) base de L

$$\text{Tr}(e \cdot g e) = \begin{cases} 0 & \text{si } g \neq 1 \\ 1 & \text{si } g = 1 \end{cases}$$

Il n'est pas commode de rester dans le cadre des extensions de corps.

"G-algèbre galloienne"

$n \geq 1$; K corps de base, G groupe fini, $|G| = n$

Une K -algèbre commutative L munie d'une action de G

conditions 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 -torsor sur K (espace principal homogène à droite sur G)

[L sert à l'ordre des objets où opère G .]

(17)

③ L est une K -algèbre étale de rang n , et l'action de G sur $\Omega(L) = \text{Hom}^{\text{alg}}(L, K_S)$, K_S étant séparable, est simplement transitive.

$\Omega(L)$: ensemble à n éléments, avec action de $G_K = \text{Gal}(K_S/K)$ à gauche, action à droite de G , 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, extérieurs galociennes de degré fini de K , permutes par G .

Réclame:

① ext. des scalaires L/K G -gal
 L'/K ext., $L \otimes_K L'$ G -alg. gal.

② Induction:

S: $\varphi: G \rightarrow G'$ est un homomorphisme de groupes finis, toute G -algèbre galocienne définit une G' -algèbre galocienne induite L'

Le couple formé de $L' \rightarrow L$ compatible avec l'action de G
 $(L' \text{ et } L' \rightarrow L)$ sont déterminés à isom. unique

HCG, alg. ind: $\text{Ind}_H^G(K_H)$

(179)

Pour toute G -algèbre galoisienne, il existe un s/g H de G (déf: à conj. près) et une ext. gal. K_H de K à groupe de Galois H , telle que $L = \text{Ind}_H^G(K_H)$.

classes d'isom. de G -alg. gal. \longleftrightarrow repr. gal. dans G
hom. (à conj. près)
 $f: G_K \rightarrow G$

Opérations de changement de base ① et ②:

① K'/K $G_{K'} \rightarrow G_K \rightarrow G$

② Induction $G_K \rightarrow G \rightarrow G'$

Question:

Peut-on donner un critère pour l'existence d'une "bonne base" pour G -alg. gal. L ?

Plus généralement:

G - forme quadratique $\stackrel{?}{\equiv}$ forme unité?

Condition nécessaire:

(V, q) repr. de G de $V \simeq$ repr. régulière $(*)$

Lemme:

Si K est algébriquement clos, $(*) \Leftrightarrow$
forme unité'.

$$e \in V, \quad q(e, g e) = 0 \quad g \in G, \quad g \neq 1$$

$$q(e, e) = 1.$$

forme quadratique $q_g(x) = q(x, g x)$ $\frac{n-1}{n-1}$ 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 $g^* = g^{-1}$

$$\sum a_g g \mapsto \sum a_g g^*$$

V base $(g e)$ $e \in V$

Automorphisme $u: e \mapsto \sum a_g g e$

u respecte la forme quadratique \Leftrightarrow

$$(\sum a_g g)^* (\sum a_g g) = 1, \quad \text{i.e. } u^* u = 1.$$

Conclusion:

toute G - forme quadratique s'obtient de la
une telle 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 $\rho: G_K \rightarrow G$.

$$G_K \rightarrow G \rightarrow U_G(K)$$

1-cocycle

La classe de cohomologie $u_L \in H^1(K, U_L)$ attachée à L est la classe du cocycle $G_K \rightarrow G \rightarrow U_G(K)$.

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'une tension 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 tensoirs

$L \hookrightarrow P$ "torsion" ($= \text{Spec } L$)

X_P : bord. de X par P

Donet de L : $G_K \rightarrow G$

On a un 1-cocycle $G_K \rightarrow G \rightarrow \text{Aut}(X)$

Th : Si L a une belle base, et si les
tensoirs sont de degré 2, alors $X_P \approx X$.

$v, v_\alpha \rightarrow$ algèbre à involution R
 $U_R = \text{Aut}(v, \alpha)$

$G \rightarrow U_R(K) \subset R$

$K[G] \rightarrow R$ compatible à l'involution

$U_G \rightarrow U_R$

le cocycle " ζ " 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 co-j. près) tel que $s^2 = 1$

$G_K \rightarrow G$ trivial ou inv.

belle base existe $\Leftrightarrow s = 1$.

$s \neq 1$, forme trace de ζ à des signes + et -
en fait $\cong \langle 1, \dots, 1, -1, \dots, -1 \rangle$
 $\frac{n}{2} \quad \frac{n}{2}$

$(\zeta \cong \mathbb{C} \times \dots \times \mathbb{C})$
 $\frac{n}{2}$

$s = 1 \Leftrightarrow \zeta$ est (totalement) réel

Remarque:

S: l'ordre de G est pair, alors il existe (sur TR) des G -algèbres galoisiennes sans belle base.

Théorème:

Supposons que $\text{cd}_2 K \leq 1$. 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 $G_K \rightarrow G$ est contenue dans tout s/g d'indice 2 de G

(2) Pour tout $z \in H^1(G, \mathbb{Z}/2\mathbb{Z})$, $z|_L = 0$ dans $H^1(K, \mathbb{Z}/2\mathbb{Z})$.

Lemma (vrai pour tout corps K)

① S: 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

$$e' = \sum_{h \in H} h \cdot e, \quad e' \in L^H$$

$$e'g = \sum_{h \in H} h \cdot g \cdot e \quad e'g \in L^H$$

On vérifie que $\text{Tr}_{L^H}(e'_s \cdot e'_t) = \begin{cases} 0 & s \neq t \\ 1 & s = t \end{cases}$
grâce à la formule:

$$\text{Tr}_{L^H} \left(\sum_{h \in H} h \cdot x \cdot y \right) = \text{Tr}_L(x \cdot y) \quad x \in L, y \in L^H$$

Autre démonstration:

forme trace de L^H : forme unité de rang $|G/H|$

formé 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'

$$K(\sqrt{d}) \quad \langle 2, 2d \rangle \quad \text{discr} = d$$

forme trace unité' $\hookrightarrow d=1$, décomposable

A montrer :

S: (1) est satisfaite, il existe une belle base.

On peut supposer que K est parfait, et que G_K est un pro-2-groupe

⇓

K est un corps de $\dim \leq 1$

(groupe de Brauer de tout ext. gal. de K est 0).

Thm (Steinberg) :

Si K est parfait, de $\dim \leq 1$, 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 $(2, \dots, 2)$ (avec action de G_K).

(Vra: 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

$(2, \dots, 2)$.

$$G \longrightarrow U_G(K)$$

$$\downarrow \quad \nearrow$$

$$U_G^\circ(K)$$

$u_L \in H^1(K, U_G)$
 provient de $u_L^\circ \in H^1(K, U_G^\circ)$, où $u_L^\circ = 0$
 par Steinberg.

Variante :

Lemma (Bruxelles, 62)

Soit K'/K une extension quadratique de
corps parfaits. Soit B réductif convexe.
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 .

$\xi \in B(K')$, $\xi \bar{\xi} = 1$ ($-$: il est non triv. de K'/K)

$\xi \mapsto g^{-1} \xi \bar{g}$, $g \in B(K')$

On peut choisir ξ semi-simple régulier
 (condition ouverte). D'où un unique tore
 maximal $T_{/K}$ contenant ξ . Mais $\bar{\xi} \in T$ aussi
 En fait, $T_{/K}$. ξ 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. irréduc. de G soient définies sur K

(par ex. K contenant les racines n ières de 1, $n = |G|$).

$$K[G] = \prod M_x$$

x car
irred.

- $x = \bar{x}$
- $x = \bar{x}$ $\left\{ \begin{array}{l} \text{repr. orthogonales} \\ \text{repr. symplectiques} \end{array} \right.$

$M_x \times M_{\bar{x}}$, involution échange les facteurs
groupe unitaire : $M_x^* \simeq GL_{n_x}$
et son $H^1 = 0$

Groupe unitaire = $O(q_x)$

H^1 = classes de f.g. de rang n_x

$G_{+} = Sp$, $H^1 = 0$

$$H^1(K, U_G) \simeq \prod_{\chi \text{ de type orth.}} H^1(K, O(q_\chi))$$

Le cas général est plus difficile, car on a des groupes unitaires sur des corps gaudes munis d'involution.

Exemple :

$$\boxed{G = A_4}, \quad A_4 / \langle (2, 2) \rangle = \mathbb{C}_3 \quad \text{coj. } \mathbb{Q}(\sqrt{-3})$$

Supposons d'abord que $\sqrt{-3} \in K$.

$$A_4 \simeq K \times \overset{\curvearrowleft}{K} \times K \times M_3(K).$$

$$U_G \simeq \mu_2 \times G_m \times O_3 \quad O_3 = O(q_3) \\ q_3 = \langle 1, 1, 1 \rangle.$$

L/K alg. g.al. à groupe $G = A_4$
 $u_L \in H^1(K, U_G)$

Composante de (u_L) ds M_2 est 0

$$G_{12} \rightarrow G \rightarrow U_G$$

$$G \rightarrow 1 \subset \mu_2$$

composante de (u_L) ds G_m est 0
 composante de (u_L) ds $O_3 \hookrightarrow$

forme quadro tique à 3 variables

$L \rightarrow K_4 = L^{A_3}$, alg. c'est de

dim 4, discriminant 1

$$q_{K_4} = \langle 1 \rangle \oplus q_{K_4}^0.$$

Si $G = A_4$, il y a équivalence entre :

① belle base

② $q_{K_4}^0 = \langle 1, 1, 1 \rangle$

③' $q_{K_4} = \langle 1, 1, 1, 1 \rangle$

③ $G_K \rightarrow A_4$ se relève en $G_K \rightarrow \widetilde{A}_4$.

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 $\sqrt{-3} \notin K$:

En 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: $G = \text{Monstre}$.

Corollaire (K corps de nombres)

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) $G_K \rightarrow A_n$ se relève en $G_K \rightarrow \tilde{A}_n$

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 des \bar{A}_n ,
 $c^2 = 1$, $c \mapsto 1$ dans A_n .

$$c = \begin{cases} 1 \\ -1 \end{cases} \text{ 'élé' non triv. de } \bar{A}_n.$$

Le relèvement $G_K \rightarrow \bar{A}_n$ peut être
modifié par un rel. $G_K \rightarrow \{\pm 1\}$.

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 :

S: L a une belle base, posons

$$K_n = L^{A_{n-1}}.$$

La forme trace est $\langle 1, \dots, 1 \rangle$.

La forme trace est $\langle 1, \dots, 1 \rangle$.
Donc $w_2 = 0$. On sait que w_2 est
l'obstruction à reléver.

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, Pernet : cas exceptionnel).

U_G° : comp. nente de U_G
 c'est un groupe réductif connexe

U_G^1 : semi-simple connexe
 (groupe dérivé de U_G°).

$$\begin{array}{c} \tilde{U}_G^1 \\ \downarrow \\ U_G^1 \subset U_G^\circ \subset U_G \end{array}$$

$u \in H^1(G_K, U_G)$, $G_K \rightarrow G \rightarrow U_G(K)$
 plongement évident.

O. a déjà vu que l'image de G
 est contenue dans $U_G^\circ(K)$

Comme $G = [G, G]$, image est contenue
 dans $U_G^1(K)$.

$$\tilde{U}_G^1(K)$$

$$\pi \downarrow$$

$$G \subset U_G^1(K)$$

$$\textcircled{3} \quad G \subset \pi \tilde{U}_G^1(K) \quad \text{En effet,}$$

$$1 \rightarrow C \rightarrow \tilde{U}_G^1 \rightarrow U_G^1 \rightarrow 1$$

$$\tilde{U}_G^1(K) \rightarrow U_G^1(K) \rightarrow H^1(K, C)$$

↑
hom

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

$$\tilde{G} = \pi^{-1}(G), \text{ isom. à } G \times C(K)$$

On a supposé $H^2(G) = 0$.

Donc G se relève

$$\begin{array}{c} \tilde{G} \subset \tilde{U}_G(K) \\ \downarrow \pi \\ G \subset U_G^1(K) \end{array}$$

$\tilde{z}_L \in H^1(K, \tilde{U}_G^1)$ est 0 ?

$G_K \rightarrow G$

$c \mapsto 1$

Un peu plus compliqué quand $G \neq [G, G]$.

Problème ouvert :

Généraliser ceu 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 :

$cd(K) \leq 2 \Rightarrow H^1(K, \text{semi-simple simple}) = 0$
converse

Dans cette direction, on a en tout cas :

Merkurjev-Suslin

$cd \leq 2 \Rightarrow D$ algèbre centrale simple/ K ,
 $K^* = \text{Nrd } D^*$.

Prochaine fois :

2-Sylow ab. il'. $\underbrace{(2, \dots, 2)}_{r \text{ factors}}$

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 bonne 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 .

Résultat des thm de Springer

(197)

$G_K \rightarrow G$ 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^o est la forme unité. $q_L^o = 2^r \otimes \langle 1 \rangle$.

D'où condition nécessaire pour l'existence d'une belle base.

② Supposons S abélien élémentaire, de type $(2, \dots, 2)$, de rang r .

Th 2: La forme q_L^o , multipliée par 2^r , est une r -forme de Pfister.

Autrement dit : si r est pair, q_L^o est une forme de Pfister, si r est impair, $2q_L^o$ 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') $2q_L^0$ $\longrightarrow \langle 1, \dots, 1 \rangle$.

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 -modèle

\mathbb{Z} p - primaire ($\text{car } p=2$) à action triviale
 de G)

199

S: S est un groupe abélien élémentaire de rang r , alors $H^*(S) = \text{Sym } H^1(S)$ = alg. de pol. en r générateurs de $d^{\circ 1}$.

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".

ζ est associé à un homomorphisme $\pi: G_K \rightarrow G$. Si $x \in H^i(G)$, $\pi^*x \in H^i(G_K) = H^i(K)$.

Je pose $x_\zeta = \pi^*x \in H^i(K)$.

En particulier, z_ζ est un élément bien défini de $H^r(K)$, indépendant du choix de ζ .

Th 5: L'invariant cohomologique dans $H^r(K)$ de la forme de Pflister $z^r q^{\circ}$ est $z_\zeta + (-1) \dots (-1) = z_\zeta + e^r$, $e = (-1) \in H^r(K)$.

r -forme de Pfister :

$$\simeq \langle 1, -\alpha_1 \rangle \otimes \dots \otimes \langle 1, -\alpha_r \rangle = \langle \langle \alpha_1, \dots, \alpha_r \rangle \rangle.$$

Soit invariant d'Arason est $(\alpha_1) \dots (\alpha_r) \in H^r(K)$

En particulier, $\langle 1, \dots, 1 \rangle$ a pour invariant cohomologique $(-1) \dots (-1) = \alpha^r \in H^r(K)$.

Corollaire : La forme $2^r q_L^r$ a même invariant cohomologique que la forme unik' n et seulement si $z_L = 0$.

On suppose w agit transitivement sur $S - \{1\}$.

Th 6 : Si $r \leq 4$ (ou si les conjectures de Milnor sont vraies pour le corps K),
L a une belle base $\iff z_L = 0$.

Exemples :

$\boxed{r=0}$ G est d'ordre impair.
 Pas de condition — tjs belle base.

$\boxed{r=1}$ Si $S = C_2$, il existe $G \xrightarrow{\cong} C_2 \rightarrow 1$

$$H^1(G) = \mathbb{Z}/2\mathbb{Z} \quad 1 \rightarrow H \rightarrow G \rightarrow C_2 \rightarrow 1$$

$$z \in H^1(G) \quad 0 \text{ ou } z_L = 0$$

$z \in H^1(G)$. On veut $z_L = 0$
belle base $\iff \pi G_K \subset H$, H d'ordre impair.

r=2

$$S = (2, 2)$$

$\text{Aut } S = S_3$, image de N/S dans

$\text{Aut } S$ 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

$$1 \rightarrow C_2 \rightarrow \tilde{G} \xrightarrow{\varphi} G \rightarrow 1$$

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 une belle base

si et seulement si $\pi: G_K \rightarrow G$ se

relève en $\tilde{\pi}: G_K \rightarrow \tilde{G}$.

S: $G = A_4$ ou A_5 , on retrouve que le relèvement à \tilde{A}_4 , \tilde{A}_5 est suffisant pour l'existence d'une belle base.

S: $G = PSL_2(\mathbb{F}_q)$, $q \equiv \pm 3 \pmod{8}$, belle base \Leftrightarrow élément possible dans $\tilde{G} = SL_2(\mathbb{F}_q)$.

Un élément $\tilde{\pi}$ définit une \tilde{G} -algèbre galoisienne $\tilde{\mathbb{L}}$.

Th 7: Il existe un choix $\tilde{\pi} \tilde{\sim}$ (non unique en général) tel que $\tilde{\mathbb{L}}$ ait une belle base.

r=3 deux possibilités pour l'action de $W = N/S$. Si transitif (sur éléments $\neq 1$) elle donne soit un groupe C_7 , soit $C_3 \cdot C_7$ (produit semi-direct, avec C_7 normal).

Exemple: $SL_2(\mathbb{F}_8)$, 2-Sylow $S = \mathbb{F}_8^*$
 $(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix})$, $N = (\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix})$, N/S opérée par $\mathbb{F}_8^* \cong C_7$.

Groupe de Janko J_1 , N agit par un groupe d'ordre 21.

(Notez 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).

$z \in H^3(S)$? Polygone de $l^{\circ} 3$.

On considère $N_{\mathbb{F}_8/\mathbb{F}_2} = N$.

C'est un polygone cubique - après choix d'une base de \mathbb{F}_8 sur \mathbb{F}_2 .

$$N(\lambda \pm) = N(\lambda) N(\pm), \quad N(\lambda) = 1 \text{ si } \lambda \in \mathbb{F}_8^*.$$

Belle base $\Leftrightarrow z_L = 0$.

Exemples de calcul de z_L .

① $G = SL_2(\mathbb{F}_8)$

“Méthode de rigidité” permet de

fabriquer des extensions de $\mathbb{Q}(\tau)$ à
groupes de Galois G , ramifiée en 3 points
(conjugué par le corps cubique de disc. g^2),
la ramification étant d'ordre 3.

Si K est de car 0, et si $t \in \text{TP}_1(K)$,
distinct des 3 points de ramification,



L_t algébre galoisienne sur K (spéc.)

D'où un invariant $z_{L_t} \in H^3(K)$.

Th : Cet invariant est $(-1)(-1)(-1) = e^3$.

Donc L_t à une belle base



-1 est somme de 4 carrés dans K .

L_t alg. gal. sur $\mathbb{Q}(\tau)$

Invariant $(-1)(-1)(-1) \in H^3(\mathbb{Q}(\tau))$.

$z_{L_t} \in H^3(\mathbb{Q}(\tau))$

J,

ramification d'ordre 2, 5, 5

$$\text{rat} \quad \mathbb{Q} \leftrightarrow \text{conj. } / \mathbb{Q}(\sqrt{5})$$

Invariant : $(-1)(-1)(-1)$.Action non transitive $r \leq 3$ facile $r = 3$, action de W par C_3

$$S = (2, 2) \oplus 2$$

$$\begin{matrix} \curvearrowleft & \uparrow \\ C_3 & \text{fixe} \end{matrix}$$

Alors $I \rightarrow H \rightarrow G \rightarrow C_3 \rightarrow 1$ Il faut que $\pi(G_K) \subset H$ (où $\pi : G_K \rightarrow G$ corr. à \hookrightarrow)et que la H -alg. gal. ait une
belle base : i.e. $G_K \rightarrow H$ se
relève en $G_K \rightarrow \mathbb{H} = 2H$.

$r > 3$ q_L^0 remplace' 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 $2^r q_L^o$ 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 $1, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_r}$

$\sqrt{\alpha_1}, \sqrt{\alpha_2}, \dots$

$$\begin{aligned} q_{L_S} &\simeq 2^r \langle 1, \alpha_1, \alpha_2, \dots, \alpha_1 \alpha_2, \dots \rangle = \\ &= 2^r \langle \langle -\alpha_1, \dots, -\alpha_r \rangle \rangle \end{aligned}$$

Autre démonstration (plus simple)

$$L_S = K(\sqrt{\alpha_1}) \otimes \dots \otimes K(\sqrt{\alpha_r})$$

produit tensoriel de $\langle 2, 2\alpha_i \rangle$.

Th 2: $2^r q_L^o$ est de Pfister

Il suffit de le voir sur K' ,

$\pi(G_F) \subset S$, L est induite d'une S -algèbre galoisienne L_S

$$q_L = q_{L_S} \oplus \cdots \oplus q_{L_S} = n \otimes q_{L_S}$$

Th 3: Si W opère transitivement sur $S - \{\pm 1\}$,
alors q_L^0 unité \Rightarrow belle base.

On peut supposer que $L = \text{Ind}_S^G L_S$,
où L_S est une S -algèbre galoisienne.

(q: il faut remplacer K par K' , $[K':K]$ impair).

$$S \subset N \subset G$$

$L_N = \text{Ind}_S^N L_S$. 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.

$$S^1 = \text{Hom}(S, \{\pm 1\}) \cong H^1(S)$$

d'ordre 2^r

$$L_S = \bigoplus L_S^\chi, \quad \dim L_S^\chi = 1$$

$$L_s = L'_s \oplus \bigoplus_{x \neq 1} L_s^x$$

L_s^x correspond à $a(x) \in K/K^{\times 2}$

$$1_x : \langle e_x, e_x \rangle = 1$$

$$s e_x = x(s) e_x$$

L_s a forme S -forme quadratique

$$2^r q_{L_s} = \langle 1 \rangle \bigoplus_{x \neq 1} a(x) 1_x$$

$$I_{-d}^N S 2^r q_{L_s} = I_{-d}^N S \langle 1 \rangle \bigoplus_{x \neq 1} a(x) I_{-d} 1_x$$

$$w \in W = N/S$$

$$I_{-d} 1_{w(x)} \simeq I_{-d} 1_x$$

$$I_{-d}^N S 2^r q_{L_s} = I_{-d}^N S \langle 1 \rangle \bigoplus I_{-d} 1_x \bigoplus_{x \neq 1} a(x)$$

On compare L_s à L_s^{def}

$$q_L^{\circ} = \sum_{x \neq 1} a(x)$$

Th 4 : Cohomologie

$$H^i(G, A)_p \hookrightarrow H^i(S, A)_p^{N/S}$$

(i.e. on
coh. de
Tate)

A est un G -module

" p ": composante p - primaire

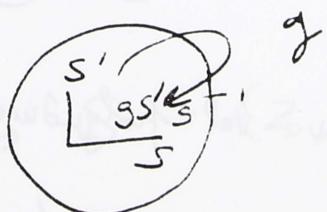
Thm : Si S est abélien et si l'action
de G sur A est triviale, alors

$$H^i(G, A)_p = H^i(S, A)^{N/S}$$

Cartan - Eckberg

"classe de cohomologie stable"

\mathfrak{z} est stable si, pour tout $s/g \in S'$ des
et tout $g \in G$, $g^{-1}sg \in S$



les classes de cohomologie de $H^i(S', A)$

obtenus à partir de \mathfrak{z} par les 2

moyens évidents : { restriction à S
restriction à S' suivie
de conjugaison

sont égales.

Quand les $Sylows$ sont abéliens, on peut supposer $g \in N$ (lemme de Burnside facile).

Th 4 : Il existe $z \in H^r(G)$ que nous donne \circ da- un sig d'ordre 2 de G .

$H^r(S)$: polyômes homogènes de d^r en r variables.

A fabriquer : polyôme 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 $(\mathbb{F}_{2^r} \rightarrow \mathbb{F}_2)$ donne un tel polyôme, soit p .

$$0 \rightarrow \text{Pol. négli} \rightarrow \text{Pol.} \rightarrow \text{Pol.}/\text{Pol. négli} \rightarrow 0$$

Pol. négli = pol. dont toutes les valeurs sur \mathbb{F}_{2^r} sont 0.

(Idéal des pol. négli. est engendré par les polyômes $x_i x_j (x_i + x_j) = x_i^2 x_j + x_i x_j^2$)

$f \in \text{Pol}/\text{Pol}_{\text{rig}}$ invariant par W

W est d'ordre impair

Donc f est image d'un polygone invariant.

Variante: $\sum_{w \in W} w(f)!$

Th 5 : l'invariant d'Arason de $2^r q_L^o$ est
 $2_L + (-1) \dots (-1)$

Il suffit de le voir sur K' , auquel cas

$q_L^o = q_{L_S}$. On est ramené au groupe S

$$L_S = \bigoplus L_S^X$$

$\pi: G_K \rightarrow S = (2, \dots, 2)$

π correspond à $x_1, \dots, x_r \in H^r(K)$

Invariant d'Arason cherché est

$$(-x_1) \dots (-x_r) \in H^r(K)$$

D'autre part, calculer l'image de t

$$(-x_1) \cdots (-x_r) = \pi(e^r(x)) \quad e = (-1)$$

$$= e^r + \sum_{i=1}^r e^i \sum_{j_1 < \cdots < j_i} (x_{j_1}) \cdots (x_{j_i})$$

On peut prendre pour f

$$f = \sum_{i=1}^r \sum_{j_1 < \cdots < j_i} (x_{j_1})^{r-i+1} (x_{j_2}) \cdots (x_{j_i}).$$

$$(\text{mod } 2, x^m = x^{m \geq 1}).$$

$$\pi^*(x)^m = (-1) \cdots (-1) (x) = e^{m-1}(x)$$

$$\text{car } (x)(x) = (-1)(x) = -x$$

Donc λ^1 invariant est $e^r + \pi^*(p)$

Th 7 $r=2$ W agit par ζ

$$1 \rightarrow C_2 \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

belle base pour $L \iff \pi$ élitable de \tilde{G}

D'où $\zeta \in \tilde{L}$

Le 2-sig de Sylow est Q_8 .

Proposition: La forme $q_{\mathbb{Z}}^o$ (de rang 8)
est une 3-forme de Pfister de type
 $\langle\langle -1, -1; \alpha \rangle\rangle$.

(i.e. $\langle 1, 1, 1, 1, \alpha, \alpha, \alpha, \alpha \rangle$).

On étend les scalaires à K' de
façon que $\tilde{\pi}(G_K) \subset \tilde{S}$.

inv. de l'élé. central
d'ordre 2

anti-invariants

$$M = M^+ \oplus M^-$$



$$\langle 1, \dots, 1 \rangle$$



$$\langle \alpha, \dots, \alpha \rangle.$$

Descente à K : de la préserve.

Proposition
belle base pour $\mathbb{Z} \iff q_{\mathbb{Z}}^o \propto \langle 1, \dots, 1 \rangle$

$\iff \alpha$ est une somme de 4 carrés

$$\iff \underbrace{(-1)(-1)(\alpha)}_u = 0 \text{ dans } H^3(K).$$

$$\iff \underbrace{(-1)(-1)(\alpha)}_u = 0 \text{ dans } H^3(K).$$

$$\tilde{Z} \mapsto u = (-1)(-1)(\alpha) \in H^3(K)$$

On peut modifier \tilde{Z} par $G_K \rightarrow (\pm 1)$
 $\gamma \in H^1(K)$.

Modification par $x \in H^1(K)$ change
 $(-1)(-1)(\alpha) \mapsto (-1)(-1)(\alpha x)$

On prend $x = \alpha$: obstruction devient 0.
 mod $\boxed{4}$

Fin du cours