

# 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

N° Cote : PB 929 9 am
<b>Institut Henri Poincaré</b> <b>BIBLIOTHÈQUE</b> 11, rue P.-et-M.-Curie 75231 PARIS CEDEX 05
N° Inventaire : 28659 B





# Annuaire du Collège de France

## Résumé des cours 1990-1991

- 4 FEV. 2000

### Algèbre et géométrie

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

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

#### §1. Notations

- $k$  est un corps commutatif, supposé de caractéristique  $\neq 2$ , pour simplifier ;
- $k_s$  est une clôture séparable de  $k$  ;
- $\text{Gal}(k_s/k)$  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 Galoisienne*, 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

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

L'un des thèmes du cours a été d'explicitier 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  $\geq 0$ , 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  $\leq 2$  ».

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  $\geq 4$  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  $\text{Spin}(q) \rightarrow SO(q)$ . 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 $H^3(k, \mathbb{Z}/2\mathbb{Z})$ : le cas du groupe spinoriel

Soit  $q$  une forme quadratique non dégénérée sur  $k$ , et soit  $x$  un élément de  $H^1(k, \text{Spin}(q))$ . 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

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

construit par Arason (qui est en fait un isomorphisme, cf. n° 2.3), on obtient un élément de  $H^3(k, \mathbb{Z}/2\mathbb{Z})$  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

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

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

Prenons pour  $G$  un groupe semi-simple *simplement connexe* déployé, et choisissons une représentation irréductible  $\rho$  de  $G$  dans un espace vectoriel  $V$  de dimension finie. Supposons  $\rho$  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  $\tilde{\rho} : G \rightarrow \text{Spin}(q)$ .

En utilisant (3.1.2) on déduit de là une application

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

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  $\rho$  la représentation fondamentale de degré 7 de  $G_2$ , l'application  $i_\rho$  correspondante est une bijection de  $H^1(k, G_2)$  sur le sous-ensemble de  $H^3(k, \mathbb{Z}/2\mathbb{Z})$  formé des éléments décomposables (cup-produits de trois éléments de  $H^1(k, \mathbb{Z}/2\mathbb{Z})$ ).



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  $H^3(k, \mathbb{Z}/2\mathbb{Z})$  que nous venons de définir. Soit  $\rho$  une représentation irréductible quelconque de  $G_2$  ; il lui correspond d'après (3.2.1) une application

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

On désire comparer  $i_\rho$  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  $\rho$ , écrit comme combinaison linéaire des poids fondamentaux  $\omega_1$  et  $\omega_2$  ( $\omega_1$  correspondant à la représentation de degré 7, et  $\omega_2$  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  $\text{Kill}_x$  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  $\text{Kill}_x$  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  $x_3 \in H^3(k, \mathbb{Z}/2\mathbb{Z})$  (obtenu par (3.2.1) grâce à la représentation irréductible  $\rho$  de dimension 26 de  $F_4$ ), et un élément  $x_5$  de  $H^5(k, \mathbb{Z}/2\mathbb{Z})$  de la forme  $x_5 = x_3 y z$  avec  $y, z \in H^1(k, \mathbb{Z}/2\mathbb{Z})$ .



(3.4.2 - « *invariant mod 3* ») Un élément de  $H^3(k, \mathbb{Z}/3\mathbb{Z})$ , 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  $\mathbb{Q}(T)$ ), 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  $\geq 3$ ) mod 2, mod 3 et mod 5 (car 2, 3, 5 sont les *nombre 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  $i_p : H^1(k, E_8) \rightarrow H^3(k, \mathbb{Z}/2\mathbb{Z})$  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  $H^1(k, \mathcal{O}(q_1)) \rightarrow H^1(k, \mathcal{O}(q))$  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  $H^1(k, O(q)) \rightarrow H^1(k', O(q))$  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  $H^1(k, O(q)) \rightarrow H^1(k, O(q \otimes q'))$  lorsque le rang de  $q'$  est impair (le morphisme  $O(q) \rightarrow O(q \otimes q')$  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

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

Notons  $q_A^\circ$  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  $q_A^\circ$ . Il y a deux cas à distinguer :

(5.1.1)  $n$  est impair.

Les formes  $q_A$  et  $q_A^\circ$  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  $\text{PGL}_n \rightarrow \text{SO}_n$  donné par la représentation adjointe et en montrant, par un calcul de poids et racines, que cet homomorphisme ne se relève pas au groupe  $\text{Spin}_n$  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  $e : \text{Gal}(k_s/k) \rightarrow S_6$  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  $e' : \text{Gal}(k_s/k) \rightarrow S_6$  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  $q_{E'} \approx 2q_E$  (mais pas  $q_{E'} \approx q_E$  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  $\varphi_L : \text{Gal}(k_s/k) \rightarrow G$ , défini à conjugaison près.

Lorsque  $\varphi_L$  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  $\varphi_L$  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  $\varepsilon_L$  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  $\leq 1$  (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  $2^r m$ , avec  $m$  impair.



(6.5.1) - Il existe une  $r$ -forme de Pfister  $q_L^1$ , et une seule à isomorphisme près, telle que  $2'q_L \approx m \otimes q_L^1$  (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  $H'(G, \mathbb{Z}/2\mathbb{Z})$  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  $H'(k, \mathbb{Z}/2\mathbb{Z})$  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  $H'(k, \mathbb{Z}/2\mathbb{Z})$ .

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  $\text{PSL}_2(\mathbb{F}_q)$  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  $\varphi_L : \text{Gal}(k_s/k) \rightarrow G$  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  $\text{SL}_2(\mathbb{F}_8)$  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  $2^r$ . 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  $b$  parcourent  $H^1(G, \mathbb{Z}/2\mathbb{Z})$ .

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 étales de la droite affine en caractéristique  $p$*  (C.R. Acad. Sci. Paris, 311, 1990, série I, 341-346).  
 — *Spécialisation des éléments de  $\text{Br}_2(\mathbb{Q}(T_1, \dots, T_n))$*  (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  $\theta$ -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

pages

1	Definitions
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 $\delta x = x^2$
25	Classes de cohomologie négligeables
26	Une formule de cobord
31	$\text{Br}_p K$ en caract. $p > 0$
34	Invariants cohomologiques des formes quadratiques
36	Un autre invariant (rang pair $\geq 4$ , disc. = 1)
41	$K^*/ND^* \rightarrow H^3(K)$ d'après Mercurier-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 $\delta^1$ et $\delta^2$
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 de  $H^1$
- 91 Théorème de simplification d'Arason-Pfister ( $q \mapsto q \otimes q'$ ,  $\text{rg } q'$  impair)
- 92 \_\_\_\_\_ de Witt
- 94 \_\_\_\_\_ de Springer
- 100 Questions
- 101 Forme trace : cas des algèbres centrales simples ; p. 102 : alg. de rang 2
- 111 Retour à  $G_2$  : table
- 112 Produit tensoriel de 2 algèbres de quaternion
- 114 Puissances divisées (si  $-1$  est un carré)
- 118 Forme trace des corps et des algèbres étales
- 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° degré
- 140 Le cas de  $A_6$  ; l'invariant dans  $H^3(K)$  ?
- 142 Automorphisme externe de  $A_6$  ; la formule  $q'_E \simeq 2q_E$
- 145 Retour sur l'équation du 5° 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 tenseurs quadratiques
- 165 Le théorème de Bayer-Lust
- 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 Bayer-Lustha
  - 184 Le cas où  $cd_2 K \leq 1$
  - 188 Parenthèse sur l. structure de  $U_G$
  - 191 Le cas où  $K$  est un corps de 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  $\mathbb{Q}(T)$ Rappel de définitions $K$  corps,  $\overline{K}$  clôture algébrique $\downarrow$   
 $K_s$  clôture séparable $\downarrow$   
 $K$  $G_K = \text{Gal}(K_s/K)$  groupe profini  
 $= \varprojlim \text{groupes finis.}$ 1er contexte $A$  groupe abélien où opère  $G_K$  (continument)  
(fixateur dans  $G_K$  d'un élément de  $A$  est ouvert). $G_K$ -module.On définit  $H^i(G_K, A) = \varinjlim_U H^i(G_K/U, A^U)$  $U$  s/g ouvert normal de  $G_K$  $H^i$ : foncteurs dérivés du foncteur "points fixes"  
rel au 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<sup>ème</sup> situation

A groupe,

A non nécessairement commutatif ou opère  $G_K$

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

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

G groupe qui opère sur A

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

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

$$= a_s s a_t$$

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

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

c'est un ensemble point.

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  $\Gamma$  un groupe fini

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

$\rho$  repr. irréd. /  $\mathbb{C}$  de  $\Gamma$   
caractère à valeurs dans  $K$

Peut-on la réaliser sur  $K$ ?

Sinon, pourquoi?

$\rho$  isom. aux  $s\rho$ ,  $s \in G_K$

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

Est-ce que

$$A_{st} = A_s^{-1} A_t ?$$

Si oui, on peut remplacer  $\rho$  par  
 $\rho'$  tel que  $s\rho' = \rho'$ .

Ce n'est pas tout à fait vrai, mais

on a  $c_{st} A_{st} = A_s^{-1} A_t$   $c_{st} \in K_s^*$

$c_{st}$  est un 2-cocycle.

Sa classe dans  $H^2$  est obstruction  
au problème.

Notation:  $H^2(G_K, K_s^*) = H^2(K, G_m)$

Teichmüller ~ 1940

$L$   
 $|$   $G$   
 $K$

extension galoisienne finie

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



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

Weil 1951 corps de classes sous forme  
cohomologique

Artin - Tate

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

"Torsion galoisienne"  
Généralisée  
~~Développée~~ par Grothendieck : descente  
générale  
topologie étale  
~ 1958

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

Progrès dans le cas semi-simple :  
Steinberg 1965 corps <sup>(parfait)</sup> de dim. coh. 1  
 $H^1(K, U) = 0$  si  $U$  semi-simple  
connexe

Chernossor 1989  
 $H^1(K, E_8) = 0$   $K$  corps de  
nombres

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

# Références

L N S

Cohomologie non abélienne:

M. Kneser, Tata Institute

(Jacobson : coh. gal. déguisée)

I. Satake

Cohomologie abélienne

G. Poitou, Coh. gal. des modules linéaires

Dunod, 1967

S. Shatz, Profinite groups, ...

Princeton, 1972

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

J. Milne, Etale Cohomology (1980)

J. Milne, Duality theorems (~1986)

H. Koch

Platonov, Principe de Hasse

(à paraître).

Etude du  $H^1(K, \text{groupe semi-simple})$

$K$  quelconque ??



Cas orthogonal:

progress grâce à Pfister, Merkurjev - Suslin,  
Arason, Rost, Jacob, ...

Groupes exceptionnels ?

Questions:  $G_1 \rightarrow G_2$

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

Exemple:  $G_2 \hookrightarrow SO_7$

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

$$x \mapsto (x \otimes x \otimes x) = x \otimes 1_3$$

Injectif (Pfister)

Démonstration par systèmes de racines ??

$$\begin{array}{c} K' \\ | \text{ lin. } \\ K \end{array}$$

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

"

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

est-ce que  
c'est injectif ?

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

B-Lenstra: Même énoncé pour groupes  
unitaires

$$E_6, E_7, E_8$$

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

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

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

$$K_2 = K_1((T_2))$$

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

- - -

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

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

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

à coeff. dans  $\mathbb{Z}/p\mathbb{Z}$

$$H^1 \text{ a comme base } x_1, \dots, x_n \quad \dim n$$

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

Problème:

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

$$F_4, E_6, E_7, E_8 ?$$



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

(8)

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

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

(cup produit)

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

$\Leftrightarrow$  3-formes de Plücker

$\Leftrightarrow$  éléments décomposables.

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

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

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

LN 5: ces  $H^1$  sont finis.

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

Rappels :

$$\begin{array}{c} L \\ | \\ K \end{array} \quad \text{galoisienne}$$

$$K \quad \text{"objets"} \quad X \quad \text{sur } K$$

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  $a_s \in \text{Aut}_L X_0$

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

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

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

$\varphi$  modifié par un automorphisme de  $X_{0L}$   
remplace  $a_s$  par un cocycle cohomologue

Injectivité : facile

Surjectivité : pas très vrai, il faut supposer  
quasi-project. pour var. alg.



descente de Weil.

Classes d'objets sur  $K$  qui sont  $K_S$ -ison.

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

Exemples :

Formes quadratiques non dégénérées ( $\text{car} \neq 2$ )

$$X_1^2 + \dots + X_n^2$$

$$X_1 X_2 + \dots + X_{n-1} X_n \quad (n \text{ pair})$$

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  $\text{car } 2$  ( $n$  impair)

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

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

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

(11)

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

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

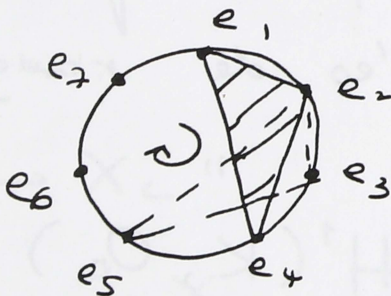
$O_n$   $n$  impair

$$\det : O_n \rightarrow \mu_2, \quad SO_n = \ker(\det)$$

$SO_n$  est lisse.

classes d'octonions (= oct. de Cayley)

(car  $\neq 2$ )



$$e_0 = 1$$

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

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

$$e_2 e_4 = -e_4 e_2 = e_1, \quad e_4 e_1 = -e_1 e_4 = e_2$$

Mêmes règles pour tous les triangles.

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

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





$$H^1(K, PGL_n)$$

$$1 \rightarrow G_m \rightarrow GL_n \rightarrow PGL_n \rightarrow 1$$

$$H^1(K, PGL_n) \xrightarrow{\Delta} H^2(K, G_m)$$

$a_s$  : 1-cocycle  $PGL_n$

$b_s$  : relèvement dans  $GL_n$

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

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

On obtient ainsi

$$Br(K) \longrightarrow H^2(K, G_m)$$

Thm C'est un isomorphisme.

### Produits croisés

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

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

chaque fibre  $\pi^{-1}(s) = E_s$  est un  
 espace principal homogène (torseur)  
 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  $E_\gamma$  se prolonge  
 $K$ -linéairement en une structure  
 d'algèbre sur  $\tilde{E}_\gamma$ .

Algèbre centrale simple, assoc.  $\gamma$

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

Cocycle se tue après ext. à  $L$

→ vrai en général.

$$\text{Br}(K) \xleftarrow{\sim} H^2(K, G_m).$$

id. usuelle

(produits croisés)

On a un précédent

$$\text{Br}(K) \xrightarrow{\Delta} H^2(K, G_m)$$

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

3<sup>ème</sup> définition : Milne

Giraud

Grothendieck utilise l'identification par  $\Delta$ .

# 1<sup>er</sup> Chapitre : Rappels sur les formes quadratiques

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

$$\text{Lies } \bar{\alpha} \quad H^i(K, \mathbb{Z}/2\mathbb{Z}) = H^i(G_K, \mathbb{Z}/2\mathbb{Z})$$

$$\text{Notation} \quad = H^i(K).$$

$H^1$  : suite exacte de Kummer

$$1 \rightarrow \mu_n \rightarrow G_m \rightarrow G_m \rightarrow 1 \quad \text{car } K \nmid n$$

$$H^1(K, G_m) = 0, \text{ donc on trouve}$$

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

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

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

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

Notation additive

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

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

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

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



On choisit l'identification "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

$f \quad g$

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

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

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

$$a \in K^*, b \in K^* \longrightarrow \begin{matrix} (a) \vee (b) & = & \text{classe de} \\ \text{"} & & \text{l'alg. quat} \\ (a)(b) & & (a, b) \end{matrix}$$

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

calcul. Plus intéressant de le faire pour  $n$  quelconque :

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

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

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

$\downarrow$   
 $\chi$

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

construire algèbre centrale simple

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

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

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

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

On a :  $(b) \cdot (\chi) = -d([b])$

↖ Signe -



## Correction à l'Historique :

- Il faut parler de Kneser et Harder pour la nullité de  $H^1/K$  total imag. s. connexe ( $\neq E_8$ )
- Cas des variétés abéliennes (et c. eff.)

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

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

## Autres corrections

$L/K$  cyclique d'ordre  $n$

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

$$b \in K^*$$

$$[b] \in H^2(L/K, L^*) \hookrightarrow \text{Br}_m(K) = H^2(K, \mu_m)$$

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

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

$$[b]_x \stackrel{?}{=} \pm (b) \cdot \chi \quad \text{ds } H^2(K, \mu_n)$$

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

Signe correct : —

Preuve :

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

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

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

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

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

$d^0 \circ \delta = 0$ . (les 2 classes commutent)



On a :

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

(19)

Lemme :  $0 \rightarrow M_m \rightarrow M \xrightarrow{m} M \rightarrow 0$ ,  $M$   $G$ -module  
(ici  $M = \overline{K}^*$ )

On se donne

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

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

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

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

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

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

"

$$(-i(\delta m \cdot \chi))$$

le résultat souhaité s'en déduit

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

$\delta\chi$  est représenté par le cocycle

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

$\delta m$  On choisit  $x \in M$  avec  $mx = m$

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

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

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

"

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

( $\Delta \chi$  à valeurs ds  $\mathbb{Z}/m\mathbb{Z}$ , pour distribuer la parenthèse, il faut utiliser  $F$ ).







$k$  commute aux ext. de scalaires

$\alpha$  1-cocycle ds  $\text{Aut } D$ ,  $D \in C_1$

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

$\Delta$  par torsion à partir de  $D = M_2$

$$F(\Delta) = {}_\alpha F(D)$$

$$F(D) = P_1$$

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

$\text{Im } x = L$  droite

( $\hookrightarrow P_1$ )

, d'où  $F(\Delta)$  est un  $P_1$  tordu.

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

Intrinsèquement (pour chx coord, cf + hr)

On fabrique un fibré  $E$  vectoriel de rang 2 sur  $C$   
 $D = \text{End}_k(E)$ .

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

Si  $P_1$ ,  $E$  décomposable.

Construction de  $E$ :

$C \times C$

$\Delta$  diagonale

$\sigma_{C \times C}(\Delta)$  fibré de rg 1  
 (fctns ayt au + un pôle simple sur  $\Delta$ ).

$\downarrow \pi = \text{pr}_1$

$$E = \pi_* \sigma_{C \times C}(\Delta)$$

$$(\mathcal{R}^1 \pi_* = 0)$$

La fibre en  $P$ ,  $E_P =$  fctns rationnelles sur  $C$  ayt au plus 1 pôle simple en  $P$ ,  
 est de dimension 2.

$$0 \rightarrow \underset{\substack{\text{(fibré trivial)} \\ \text{de rg 1}}}{1} \rightarrow E \rightarrow \underset{\text{fibré tgr}}{T} \rightarrow 0.$$



$$H^1(C, \text{Hom}(\tau, 1)) = H^1(C, \Omega')$$

(22)

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

(Prob'  $\pm 1$ , car sinon on aura des ennus dans la caract correspondante à ce nbre, ce qui n'est pas).

$$\text{Si } C = \mathbb{P}, \quad E = \mathcal{O}(-1) \oplus \mathcal{O}(-1) \\ D = \text{End}_K(E) = M_2$$

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

Formules évidentes

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

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

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

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

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

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

Débouche sur la  $K$ -théorie de Milnor...



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

(23)

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

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

$$\delta x = 0.$$

opération  
de Bockstein  
(modulo  $p$ )  
 $= Sq^1$  (fais. de Steenrod)

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

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

$X$  cplète simpl. par ex.  
 $i, A$  fixé

On veut trouver une formule pour  $H^i(X, A)$ ...

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

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

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

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

$$\text{ici } \mathbb{S}_N / \pm 1 = \mathbb{P}_N(\mathbb{R})$$

$\mathbb{S}_N$  : sphère

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

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

" $N = \infty$ " 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  $z \in H^1$

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

$$\delta z = \begin{cases} 0 \\ z^2 \end{cases} \quad \text{mais si } 0, \text{ ce serait} \\ \text{Donc c'est } z^2. \quad \text{vrai toujours (impossible)}$$

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

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

$C_2$  gr. cycl. d'ordre 2

$$G_2 \xrightarrow{f} C_2$$

$$x = f^*(z)$$

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

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

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

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

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

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

$$\delta x = 0$$

# Classes de cohomologie "négligeables"

(25)

$G$  fini,  $M$   $G$ -module

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

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

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

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

Exemples: , en cohom modulo 2

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

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

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

si  $G = (2, \dots, 2)$

$H^*(G) = \text{alg. de polyn eng. par } m \text{ élt de degré 1.}$

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  $K = 2 \Rightarrow H^i(K) = 0$  si  $i$  pair de 2

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

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



Quelques remarques "négligeables"

• Dans le cas des 2-gps, les classes nég st l'ideal engendré par  $(v^2v + uv^2)$

• Si  $K$  car  $p$ ,  $p \equiv 1 \pmod{4}$

(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  $y \in H^2(G)$ ,  $\delta y$  est négligeable  
 $\uparrow$   
 $H^3$

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

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

Une formule de cobord.

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

suite exacte de  $G$ -modules

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

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

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

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

et



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

Formule:  $\delta_x(x) = \delta(x) + \langle \chi, x \rangle$   
 $x \in H^i(G, C) \quad \langle \chi \rangle \in H^1(G, \text{Hom}(C, A))$   
 $C \times \text{Hom}(C, A) \rightarrow A.$

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

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

$\delta_x$   $\mapsto f(s_1, \dots, s_{i+1}) - \dots$

$\delta_x(x) - \delta(x)$  repres. par le cocycle

$s_1, \dots, s_{i+1} \mapsto \chi_s, (\wedge^i f_c(s_2, \dots, s_{i+1}))$   
 $\parallel$   
 cup-produit

Applications (car  $K \neq 2$ )

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

$$0 \rightarrow \mu_2 \rightarrow \mu_4 \rightarrow \mu_2 \rightarrow 0 \quad (*)$$

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

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



$$\delta_{(*)}^i: H^i(K, \mu_2) \rightarrow H^{i+1}(K, \mu_2)$$

$\delta_{(*)}^i$  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  $p$  premier  $\neq 2$ , car  $K \neq \mathbb{R}$ .

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

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

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

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

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

L'action de  $G_K$  sur  $\mu_{p^2}$  définit  $\varphi: G_K \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^* \cong \mathbb{Z}/p\mathbb{Z}$   
 le unique homomorphisme qui applique la classe modulo  $p^2$  de  $1+2p$  sur  $1 \bmod p$ .

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

$$\frac{m^{p-1} - 1}{p} \equiv -\varepsilon(m) \bmod p.$$

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

2 preuves : Il suffit de prouver cette formule



quand  $K$  contient  $\mu_p$  (car  $K' = K(\mu_p)$   $K$  de  $d^{\circ} 1^{\text{er}} \text{ à } p$  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  $0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$ .

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

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

$$\begin{cases} \mu_p = \mathbb{Z}/p\mathbb{Z} \text{ via } z \\ \varphi \text{ rend l'action de } \mu_p \\ z^p = z \end{cases} \quad s \in G_K : s \cdot z = z^{1+s(p)} = z \cdot z$$

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

Autre preuve via algèbres cycliques de  $\text{Br}_p(K)$   
 $(\varphi) = \text{classe de } (z)$ .

Corollaire  $G$  fini  $p \neq 2$

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

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

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

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

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

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

$H^0$	$1$	$H^2$	$\delta u$	$H^3$	$u \cdot \delta u$	$H^4$	$\delta u \cdot \delta u \dots$
$H^1$	$u$						



Compléments

## 1) Coh. "négligeable"

$$x \in H^i(G, V) \quad G \text{ fini}$$

$$K \xrightarrow{G_K} G$$

$$\text{Gal}(K_s/\mathbb{K})$$

$$\varphi^* x = 0$$

Y

$$\downarrow G$$

$$H^*(G) \rightarrow H^*(X)$$

X

$$\rightarrow BG$$

Analogue:

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

BG  
 "classifiant  
 du gpe G"

sa cohom est celle de G.

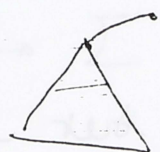
d'où le résultat pour la top. usuelle.

Pour "étale"

X complexe simplicial fini

$\exists$  esp. alg.  
 (affine)

/  $\mathbb{C}$  qui a le même  
 type d'homotopie  
 que X.



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

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

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

Ex

$$X: \text{---}$$

$$x_1, x_2 \quad x_1 + x_2 = 1$$

$$x_i \geq 0$$

$X_0$

plan complexe a 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  
 & var de Giefel.



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

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

$$V_{N,n} \quad GL_n \text{ opère librement sur } V_{N,n}$$

$$G \subset GL_n$$

$$G \text{ opère librement sur } V_{N,n}$$

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

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

$N$  grand: pas de classes négligeables!

Mais:  $Y \downarrow G \downarrow X$   $X$  négligeable  
la classe de  $X$  se tue sur un ouvert de Zariski assez petit

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

Décider  $\text{Br}_p K$ ?

Produits croisés cycliques

$$(1^0) \quad a \in K, \quad b \in K^* \text{ donnés}$$

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

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

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

$$\begin{array}{c} K_a \\ | \mathbb{Z}/p\mathbb{Z} \\ K \end{array}$$

$$[a, b) = 0 \iff b \text{ est une norme de } K_a$$

$$\xi \in \text{Br}_p K \text{ est de la forme } [a, b)$$

$$a \text{ imposé} \iff \xi \text{ scinde (= annulé par } K_a)$$

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



$$\textcircled{2} \quad a, b \in K$$

32

$$[a, b] \in \mathcal{B}_{r_p} K$$

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

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

$$\Omega^1 K \quad \text{1-formes} \quad \sum a_i db_i \\ \text{avec } a(a_i db_i) = (aa_i) db_i \\ d(bc) = bdc + cdb$$

$$\Omega^1 K \longrightarrow \mathcal{B}_{r_p} K$$

$$\sum a_i db_i \mapsto \sum [a_i, b_i] \in \mathcal{B}_{r_p} K.$$

$$\sum a_i \frac{db_i}{b_i} \mapsto \sum [a_i, b_i) \in \mathcal{B}_{r_p} K.$$

Albert, Witt, ....

C'est surjectif, les diff. exactes  $db$  donnent 0 ds  $\mathcal{B}_{r_p}$ .

$$\Omega^1 K \xrightarrow{F-1} \Omega^1 K / dK \longrightarrow \mathcal{B}_{r_p} K \longrightarrow 0.$$

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

= "inverse de l'opérateur de Cartier".

cf Witt Hamb. Abhand. 1958.

Pour  $p=2$

$$[a, b] \mapsto \text{conique corresp.}$$

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

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

3°)

C genre 0.

(33)

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

$x \in H'(\text{---} C, \Omega')$  =  $\pm$  classe  $f$  de la dualité ?

la construction est tout à fait universelle

$$x = m \in \mathbb{Z} \quad \mathbb{P}_1 / \mathbb{Z}.$$

$p$  premier  $\Rightarrow p \nmid m$

car sinon en car  $p$ , l'extension serait triviale

donc  $m = \pm 1$



# Formes quadrotiques et leurs invariants cohomologiques

car  $k \neq 2$ .

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

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

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

• langage  $e, v, V$  de dim finie, muni d'une forme  $q$   
quad. (non deg.) (à isom. près)

• langage  $f(x_1, \dots, x_n) = \sum a_{ij} x_i x_j$   $a_{ij} = a_{ji}$   $a_{ij} \in K$   
 $d = \det(a_{ij}) \neq 0$

$f \sim f'$  s'il existe une transf. inversible des  $x_i$  amenant  $f$  sur  $f'$ .  
 $(a'_{ij}) = {}^t C (a_{ij}) C$  avec  $C \in GL_n$ .

$$f \sim \sum_{i=1}^n a_i x_i^2 \quad a_i \in K^*$$

$$\begin{aligned} x \cdot x &= q(x) \\ x \cdot y &= \frac{1}{2}(q(x+y) - q(x) - q(y)) \end{aligned}$$

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

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

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

des formes à deux variables décident de cette question

$n \geq 2$   $\{a_1, \dots, a_n\}, \{b_1, \dots, b_n\}$  sont 2-voisines si

$a_i = b_i$  pour tout  $i$  sauf au plus 2 valeurs.

$$\text{et } \langle a_j, a_k \rangle \stackrel{?}{=} \langle b_j, b_k \rangle$$

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

ie le graphe des  $\langle b_1, \dots, b_n \rangle \sim \langle a_1, \dots, a_n \rangle$  est connexe (autre 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  $i$

Thème le graphe des bases orthogonales est connexe

"

Générateurs : formes à 1 variable

Relations : formes à 2 variables

Ce principe va permettre de définir des invariants

Inv. coho  $m$  : classes de Stiefel-Whitney

(cf Delzant, fin des anneaux SO).

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

$\downarrow$

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

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

$i \geq 0$ .

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

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

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

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

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

$$w_i(q) = i\text{-ème fonction symétrique élémentaire des } (\alpha_i).$$

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  $m=2$



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

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

$V, q$  e.v. quad.

alg. de Clifford  $C(V)$

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

$C(V) = \text{alg. de quat. } (\alpha_1, \dots, \alpha_m)$   $e_1^2 = \alpha_1 \quad e_1 e_2 = -e_2 e_1$   
idem sur  $\beta$  d'où l'égalité.  $e_2^2 = \alpha_2$

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

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

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

$$w_3 = w_1, w_2 \quad \sum (\alpha_i) \sum_{j < k} (\alpha_j)(\alpha_k) = 3w_3 + \sum_{j < k} ((\alpha_j)^2(\alpha_k) + (\alpha_j)(\alpha_k)^2) + (\alpha_j)(\alpha_k)(\alpha_l)$$

• 3 mod 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  $w_j, j < i$ . Plus précisément :

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

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

Autre invariant ( $m$  pair  $\geq 4$ )

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

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

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

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



Ne dépend en fait pas de l'indice qu'on laisse tomber (37)  
 $(\alpha_2)(\alpha_3) \dots (\alpha_n) \stackrel{?}{=} (\alpha_1)(\alpha_2) \dots (\alpha_{n-1})$

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

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

$$= (\alpha_1)(\alpha_2) \dots (\alpha_{n-1}) + \underbrace{(m-2)}_{\text{pair}} \text{ fois un terme}$$

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

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

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

② Cas général

d disc.  $(d) = w_i$

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

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

$K_d = K(\sqrt{d})$  d non carré

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

la forme quadratique.

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

suite exacte



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

(38)

Suite exacte des extensions quadratiques

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

Soit  $G$  un groupe ~~discret~~ <sup>ou discret</sup> profini et  $H$  un sous-groupe d'indice 2 de  $G$ ; soit  $\varepsilon: G \rightarrow \{\pm 1\}$  le caractère de noyau  $H$ .

$A$   $G$ -module

$A_\varepsilon$  module  $A$  "tordu par  $\varepsilon$ ". On a la suite exacte:

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

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

où  $a_\varepsilon \in H^1(G, \mathbb{Z}_\varepsilon) = \mathbb{Z}/2\mathbb{Z}$   
représenté par le cocycle  $s \mapsto \begin{cases} 0 & \text{si } s \in H \\ 1 & \text{si } s \notin H \end{cases}$

Rq:  $G \rightarrow G/H \cong \mathbb{Z}_2$   $H^1(G/H, \mathbb{Z}_\varepsilon) = \mathbb{Z}/2\mathbb{Z} \hookrightarrow H^1(G, \mathbb{Z})$   
si  $G$  profini, c'est un isomorph

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

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

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

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

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

$$\begin{array}{ccc} e_1 - e_2 & e_1, e_2 & \searrow \\ & & 1 \end{array}$$

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

mais l'action de groupe est une action tordue!



On a vu une formule générale la dernière fois pour les "torques"  $\rightarrow$  cet produit, ici  $a_\varepsilon \cdot x$ .

Thme (Witt) les formes de degré  $n \leq 3$  sont classées  
par  $w_0, w_2$  (dimension  
rg)

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

$n=1$   $w_1$

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

$n=3$   $q, q'$  m  $w_1, w_2$   
discrim.

$dq$  et  $dq'$  ont disc. 1.

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

$$q = \langle \alpha, \beta, \gamma \rangle \quad \lambda \in K^* \quad 2q = \langle 2\alpha, 2\beta, 2\gamma \rangle$$
$$w_2(2q) = (2\alpha)(2\beta) + (2\alpha)(2\gamma) + (2\beta)(2\gamma)$$
$$= ((2)4(\alpha))((2)+(\beta)) + \dots$$

$$w_2(2q) = (2)(2) + w_2(q)$$
$$= +(-1)(2) + w_2(q).$$

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

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

$$-q \stackrel{\sim}{=} -\alpha x^2 - \beta y^2 + \alpha\beta z^2 = \text{Norme (alg. de quarte)} \\ \text{sur les elts de trace 0.} \quad (\alpha, \beta)$$







28/11/91

(41)

 $K \text{ car } \neq 2.$  $q \quad w_i(q) \in H^i(K) = H^i(G_K, \mathbb{Z}/2\mathbb{Z})$ rang  $q \leq 3$   $w_1, w_2$  classifiantrang  $q = 4$  dis  $\square$  ( $w_1 = 0$ )  $w_2$  et  $i(q) \in H^3(K)$  classifiant $q$ dis non  $\square$  ?

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

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

$$a_2 = b_1 a_1 \\ a_3 = a_1 b_1$$

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

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

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

$$w_2(q) + (-1)(-1)$$

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

Thème  
Mercurier Sushin

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

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

(on trouve 0 si  $a$  est une  
norme)Cet homomorphisme est injectif

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



C'est faux si le disc. n'est pas  $\square$ .

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

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

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

$$w_2(\lambda q) = m_2(\lambda)(-1) + n_1(\lambda)w_1(q) + w_2(q)$$

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

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

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

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 ex où  $dq \not\sim q$  sur  $K$   
 $K = \mathbb{Q}(i) \quad \alpha, \beta \in \mathbb{R}^* \quad (\alpha, \beta) \neq 0.$

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

$\mathbb{H}$  = corps de quaternions ramif. en  $2+i$  et  $3$

$$K = \mathbb{H}(T) \quad T \text{ indét.}$$

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

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

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

Ou bien: classif. des formes

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

si les 2 formes isomorphes, ce serait hyperbolique

Or celle-ci est anisotrope. car c'est

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

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

car d'g quot = corps.  
anisotrope



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

lemme:

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

Plus généralement d'ailleurs,  $K$  val. disc avec car  $\neq 2$ ,  $\pi$  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

$w_1$

$$H^2(K) = 0$$

( $K$  fini)

$w_1, w_2$

$$H^3(K) = 0$$

(ex: corps de nbres totalt imagin; corps de fctns d'une var sur un corps fini).

$w_1, w_2$ , signatures aux places réelles

corps de nbres.

(ou p classes de Shafel Whitney...)

On peut se débar~~asser~~asser des  $(-1)$  si  $q$  forme quadratique de rang pair  $m = 2m$

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

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

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

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

$$w(R) = 1 + \begin{matrix} \text{H}^0 \\ (-1) \\ \text{H}^1 \end{matrix}$$

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

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



$$(1 + w'_1(q) + w'_2(q) + \dots) (1 + m(-1) + m_2(-1)(-1) + \dots) = 1 + w_1(q) + w_2(q) + \dots$$

$$m_2 = \frac{m(m-1)}{2}$$

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

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

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

Pour  $m=2$   $w'_2 = w_2 + (-1)(-1) + (-1)w_1$   
 $q = \langle \alpha, \beta \rangle$   $w'_2 = (-\alpha)(-\beta)$  clifford de  $(-q)$ .  
 $m=4$   $w'_1 = w_1$   
 $w'_2 = [D_q]$

$F \in K$  corps de caract  $\neq 2$   
Anneau de Witt :  $\rightarrow$  Gothenolick-Witt  
 notation (fâcheuse !)  $GrW$  ou  $\tilde{W}$ .

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

$GrW$  universel pour les fctns de formes quad. à valeurs dans les gres abéliens

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

produit = produit tensoriel.

Anneau de Witt  $W = GrW/\alpha$   $\alpha$  engendré par  $h = \langle 1, -1 \rangle$

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

$$W = W_{\frac{1}{2}} =: GrW/\alpha.$$



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

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

Relations entre  $I_F^m / I_F^{m+1}$  ?

cf Inv. Math 1970.

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

(b)  $H^m(F)$

(c)  $R_m(F) = K_m^m(F) \mid 2 K_m^m(F)$

Qu'est-ce que  $K_*^m(F)$  ? anneau gradué, engendré par des élt de  $d^0 = 1$ , relation de degré 2 ou 1.

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

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

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

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

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

On dispose de flèches

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

$\beta \searrow H^m(F)$

flèches faciles à définir,  $\alpha$  surjective.

Conjecture : Ce sont des isomorphismes



Soi pour un corps  $F$  et un degré  $n$ ,  $\alpha$  et  $\beta$  isomorphism

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

$$\beta \searrow \swarrow \bar{e}_F^n$$

$$H^n(F)$$

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

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

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

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

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

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

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

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

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

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

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

forme de rang 0.

$$\text{ou encore } \langle 1 \rangle + \langle -x \rangle$$

les 2 formes sont égales mod  $I_F^2$  :

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

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

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

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

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

trivial!

$\searrow^2 \quad H^1(F)$

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

$\swarrow^{\text{Merkuriev} \sim 1980} \quad H^2(F)$

$m=3 \quad \alpha, \beta$  isomorphismes

Merkuriev - Suslin  
Rost

preprint 1986  
— 1986

$m=4 \quad e_F^4$  existe

Jacob-Rost Inv. Math 96 1989  
Skierski Dokl. 308 1989.

On peut aussi introduire  $\begin{matrix} F_q \\ | \\ F \end{matrix}$  plus grande 2-ext. de  $F$   
(ie ext gal. à gpe de Galois un mo-2-gpe)

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

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

$\begin{matrix} !! \\ H_q^m(F) \end{matrix}$

("cohomologie  
quadrotique de  $F$ ")

Si  $\alpha: k_m \rightarrow I^m / I^{m+1}$   
 $\beta: k_m \rightarrow H^m$



Si les  $\beta$  sont surjectifs (en dim  $\leq n$ ) alors  $H_q^m(F) \rightarrow H^n(F)$  est un isom.

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

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

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

$$K_F^m \longrightarrow I_F^m / I_F^{m+1}$$

$$\downarrow$$

$$H_q^m(F)$$

$$\downarrow$$

$$H^n(F)$$

Conjecturalement, toutes les flèches sont des isomorphismes

$q, q'$  formes de rang  $n$

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

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

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

$$Q \longrightarrow [Q] \in I_F$$

Lemme  $[Q] \in I_F^3$

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

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

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

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

$$I_F^3 / I_F^4 \simeq H^3(F)$$

$$i(q, q') = \text{image ds } H^3(F)$$

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

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

$Q = q \oplus -q' \quad m=4 \dots$   
cf Lam ou l'article original de Pfister

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

Remarque  $i$  est un invariant relatif

si  $q \in I^4$  ds  $\square$   
 $q$  a Norme.

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

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  $q$ .

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

$(\pm 1)$

$Spin(q)$

revêt univers à 2 feuillets  
simplt connexe.

$\{\pm 1\} \downarrow \tilde{O}(q)$

$\downarrow \hookrightarrow O(q)$

$\subset$

$\downarrow O(q)$

$\downarrow 1$

On peut associer canoniquement à  $q$  un revêt à 2 feuillets redonnant le gpe des spineurs sur  $SO$ .

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

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

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

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

$\Rightarrow x \cdot y = -y \cdot x$  si  $x$  et  $y \perp$  pour  $q$ .

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

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

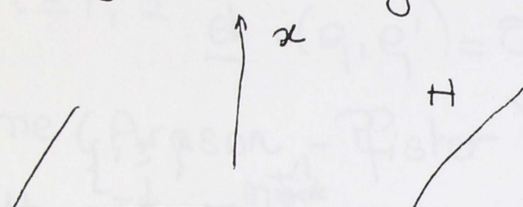
$(x_1 \dots x_k)' = x_k \dots x_1$   $x_i \in V$



# Remarque

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

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



$H = \text{orth. de } x.$

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

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

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

$$C = C^+ \oplus C^- \quad \begin{array}{l} C^+ \text{ eng. par les produits pairs} \\ x_1 \dots x_{2n} \quad x_i \in V \\ C^- \text{ ——— impairs} \end{array}$$

$C^+$  pair /  $C^-$  impair

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

$K$  Groupes algébriques sur  $K$

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

Ces groupes ont les propriétés voulues

A définir

$$\begin{array}{c} \tilde{O}(q)_+ \\ \cup \\ z \end{array} \rightarrow \text{So}(q)$$

$$v \mapsto zvz^{-1} \in \text{So}(q)$$

$$\tilde{O}(q)_- \rightarrow \text{O}(q) - \text{So}(q) \quad v \mapsto -zvz^{-1}$$



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

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

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

Si  $P$  a des vecteurs de carrés 1 pour  $q$ , ~~on~~ on  
en choisit un,  $\alpha(q) = so(q) \rtimes (1, \sigma)$   
 $\sigma$  réflex. / type perpend.

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

4/2/91

(53)

(Bruno Kahn)

I Formes de Pfister

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

$$(x_1^2 + \dots + x_n^2)(y_1^2 + \dots + y_n^2) = (x_1 y_1 - x_2 y_2 - \dots - x_n y_n)^2 + \dots$$

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

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

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

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

Si  $E = F(X_1, \dots, X_m, Y_1, \dots, Y_m)$  (2) Formule  $N(\vec{X})N(\vec{Y}) = N(\phi(\vec{X}, \vec{Y}))$

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

(fractions rationnelles)

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  $N = N_0 \circ \vec{\phi}$  avec

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

$[E:F] < \infty$   $D$  corps gauche de centre  $E$

ou

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

$$[E:F] < \infty$$

$\sigma$  "corps" d'octonions de centre  $E$ ,  $\nu_0$  norme de  $\sigma$ .

Il n'y a rien d'autre:  $\vec{\phi}$  donné par des polyn. homog. d'où donné par loi d'algèbre, si l'algèbre est associative avec éléments neutres à gauche et droite, c'est forcément alternée et ces algèbres sont classifiées.



et on autorise les dénominateurs  
 si  $d=2$  il y en a d'autres les formes de Pfister.

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

$\langle\langle a_1, \dots, a_n \rangle\rangle = \langle 1, -a_1 \rangle \otimes \dots \otimes \langle 1, -a_n \rangle$   
 c'est une  $n$ -forme de Pfister.

⚠ notation sans signe - existe ds la littérature

Théorème (Pfister)  $\varphi$  forme quadratique anisotrope  
cond. equiv.

- (1)  $E/F$  extension <sup>qge</sup>  $\varphi|_{E^n}$  est un gpe
- (2)  $\varphi$  est multiplicative avec  $\varphi(\vec{x})\varphi(\vec{y}) = \varphi(\vec{\phi}(\vec{x}, \vec{y}))$
- (3)  $\exists \vec{\phi}$  linéaire en  $\vec{y}$  avec (2)
- (4)  $\varphi$  est une forme de Pfister

(cf Lam, ch X).

On va donner une dem constructive de (4)  $\Rightarrow$  (1) et (3)  
 Par récurrence sur  $n$ .

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



$$V = W \oplus W.$$

$W$  espace  
 vect associé  
 $\otimes \varphi_{n-1}$

$\varphi_{n-1}$  forme de Pfister donc multiplicative

$x \in W \quad \exists u_x \in GL(W)$

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

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

$$x = \begin{matrix} x_0 & x_1 \\ \uparrow & \uparrow \\ W & W \end{matrix}$$

$$u_x = \begin{pmatrix} u_{x_0} & a_n u_{x_1} \\ u_{x_1}^* & v \end{pmatrix} \quad v? \in \text{End}_F W$$

$u_{x_1}^*$  adjoint



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

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

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

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

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

Pour 16 variables par exemple:

$$\begin{aligned} x_1^2 + \dots + x_{16}^2 &\xrightarrow{\det} (x_1^2 + \dots + x_8^2)^4 \\ x_1^2 + \dots + x_{32}^2 &\rightarrow (x_1^2 + \dots + x_{16}^2)^{24} (x_{17}^2 + \dots + x_{32}^2)^4 \end{aligned}$$

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

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

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

Donc  $-1 = x_1^2 + \dots + x_n^2 \quad \Delta = \Delta(F)$   
 $(\Rightarrow \forall i_1, \dots, i_n \quad x_{i_1}^2 + \dots + x_{i_n}^2 \neq 0)$

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

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

Notation  $\varphi$  forme quadratique

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

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

$\mathcal{D}_F$  est un groupe

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



# Théorie des formes de Pfister

56

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

$I_F =$  idéal de l'anneau de Witt  $\rightarrow$  contient  $\frac{1}{2}$  du moy. de l'anneau  
 $= \text{Ker} (W(F) \xrightarrow{rg} \mathbb{Z}/2\mathbb{Z})$

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

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

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

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

Corps de fonctions, de  $\text{rg } N$

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

$X_q =$  variété des zéros de  $q$   $\left\{ \begin{array}{l} \text{affine} \\ \text{projective} \end{array} \right.$

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

$$\dim F(q) = N-1$$

(cas projectif  $N-2$ )

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

$$q = \langle 1 \rangle \perp -q'_{x_2, \dots, x_n}$$

$$F(q) = F(x_2, \dots, x_n, \sqrt{q'(x_2, \dots, x_n)})$$

ie extension quadratique d'une transc. pure



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

(57)

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

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

$\Rightarrow$  lemme  $q$  anisotrope /  $F$   
 $q \otimes F(q)$  est anisotrope.

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

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

$$\text{Ker}(W(F) \rightarrow W(E)) = \langle\langle a \rangle\rangle_{W(F)}$$

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

$q$  anisot. /  $F$   $q \otimes E$  isotrope  $\Rightarrow q \geq 2 \langle\langle a \rangle\rangle$

$\sim$   
contient une  
ss forme.

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

Lemme 2 (Pfister)  $\varphi, \psi$  deux formes quadratiques  
avec  $\varphi$  anisotrope.

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

Théorème  $\varphi, \psi$  deux formes quad.,  $\varphi$  anisotrope  
dun  $\varphi > 1$

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

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

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

c) Si  $\varphi$  est de Pfister,  $\psi \simeq \varphi \otimes \theta$   
ie  $\text{Ker}(W(F) \rightarrow W(F(\varphi))) = \varphi W(F)$ .



Démonstration

(58)

$$\psi = \langle 1 \rangle \perp -\psi'$$

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

hyperbolique

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

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

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

dans le cas a)  $\psi$  est multiplicatif, donc de Pfister

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

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

Théorème d'Arason-Pfister (~ 1971)

$q$  forme quadratique de rang  $< 2^n$

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

Alors  $q$  est hyperbolique.

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

$$q \sim \varepsilon_1 \psi_1 + \dots + \varepsilon_r \psi_r \quad \varepsilon_i = \pm 1 \quad \psi_i \text{ formes de Pfister}$$

On raisonne par récurrence sur  $r$ .

Si  $\psi_r$  non hyp.,  $\psi_r$  anisotrope

$$q \otimes_F F(\psi_r) = \varepsilon_1 \psi_1 + \dots + \varepsilon_{r-1} \psi_{r-1} \text{ est hyperbolique}$$

Si  $q$  non hyperb.,  $q_{an} = \psi_n \otimes ? \Rightarrow \text{rang } q_{an} \geq 2^n$  et c'est



# Invariant cohomologique

(59)

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

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

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

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

$(a_i)$  classe de  $H^1$  via Kummer  
 $\cup$  cup produit.

## Démonstration

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

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

D'où:

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

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

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

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

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

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

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

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



Dém du 2<sup>e</sup> lemme pour  $n=2$

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

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

" (relation de Steinberg).

Dém. du lemme d'Arason

$$\begin{aligned} \psi_1 &= \langle\langle a_1, \dots, a_{m-1} \rangle\rangle \\ &= 1 \perp \psi'_1 \end{aligned}$$

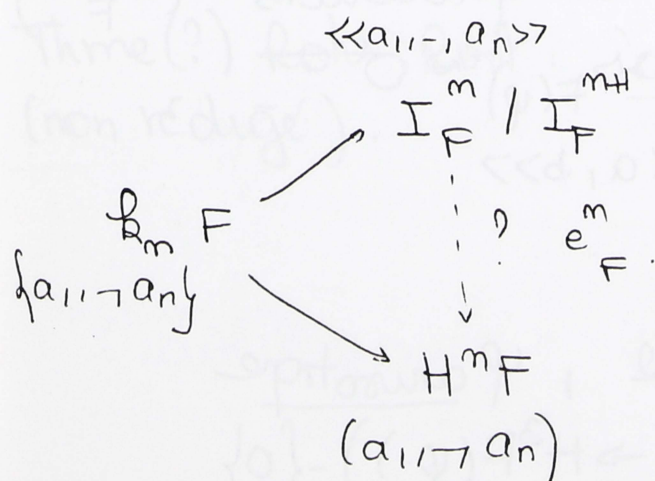
$$\begin{aligned} \psi_2 &= \langle\langle b_1, \dots, b_{n-1} \rangle\rangle \\ &= 1 \perp \psi'_2 \end{aligned}$$

Hypothèse  $\psi_1 \otimes \langle\langle a_n \rangle\rangle \perp -\psi_2 \otimes \langle\langle b_n \rangle\rangle$  est hyperbolique  
 $\Theta = (\psi'_1 \perp -\psi'_2) \perp (a_n \psi_1 \perp -b_n \psi_2) \sim 0$

Remarque  $\Theta$  forme hyperbolique de rang  $2N$ ,  $\rho \subset \Theta$   
 $\text{rg } \rho > N \Rightarrow \rho$  est isotrope.

$$\Rightarrow \exists c = a_n \psi_1(\bar{x}) = b_n \psi_2(\bar{y})$$

$$\begin{aligned} \langle\langle a_1, \dots, a_n \rangle\rangle &= \langle\langle a_1, \dots, a_{m-1} \rangle\rangle \perp c \psi_1(\bar{x}) \perp \psi_1 \\ &\sim \langle\langle a_1, \dots, a_{m-1} \rangle\rangle \perp -c \psi_1 = \langle\langle a_1, \dots, a_{m-1} \rangle\rangle \end{aligned}$$



Arason (Elman - Lam)

$\psi_1, \psi_2, \psi_3$  formes de Pfister

$$\begin{aligned} \psi_1 \perp \psi_2 &\equiv \psi_3 \pmod{I_F^{m+1}} \\ \Rightarrow e_F^m(\psi_1) + e_F^m(\psi_2) &= e_F^m(\psi_3) \end{aligned}$$



Thme (Arason)  $e_F^3$  est bien définie  $\forall F$   
 Thme (Jacob - Rost, Shwsky)  $e_F^4$  idem

(61)

Remarque (Milnor)

$$W_{2^{n-1}}(\langle\langle a_1, \dots, a_n \rangle\rangle') = \underbrace{\{-1\}^{2^{n-1} * n}}_{-1 \text{ dans } H_1} e_F^m(\langle\langle a_1, \dots, a_n \rangle\rangle)$$

Arason montre que  $e_F^n$  est bien définie  $\forall F$  si  $\forall F$   
 $\varphi$  forme quadratique de rang  $\geq 2^m$   $H^n F \hookrightarrow H^n F(\varphi)$

$m=1$   $H^1 F \not\hookrightarrow H^1 F(\varphi)$  si  $F$  n'est pas alg<sup>t</sup> fermée  
 ds  $F(\varphi)$   
 $\Rightarrow \text{rg } \varphi = 2$ .

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

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

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

$\Rightarrow \mathbb{D}$  est un corps de quaternions  $\begin{pmatrix} a & b \\ F & F \end{pmatrix}$

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

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

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

Thme (Arason)  $\varphi$   $\text{rg } \varphi > 2$ ,  $\varphi$  anisotrope

Il existe  $\alpha \in \text{Ker}(H^3 F \rightarrow H^3 F(\varphi)) - \{0\}$

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

$(a, b, c)$  conven  
 et  $\lambda$  contrainable

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



Thme (Jacob-Rost) forme de Pfister

$$\ker(H^4(F) \rightarrow H^4(F(\psi))) = e_F^4 \psi_* H^0 F$$

Il faut à montrer l'existence de  $e_F^4$ .

Conjecture de Kato:

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

$m=1$  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  
si  $n=2$

Thme (Rost - Merkurjev - Suslin) C'est un isomorphisme  
si  $n=3$  et  $m=2^r$

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



11/2/91.

(63)

$O(q)$

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

$$\text{Spin}(q) \longrightarrow \tilde{O}(q)$$

$$1 \longrightarrow \text{SO}(q) \longrightarrow O(q) \xrightarrow{\det} \{\pm 1\} \longrightarrow 1.$$

ext. centrale (non triviale) par  $\{\pm 1\}$   
si  $n \geq 2$

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

$\tilde{O}(q)$  grpe algébrique

pts sur  $K$

$C(q)$  = algèbre de Clifford

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

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

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

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

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

Cas  $n=1$

$$\text{SO} = \{1\}$$

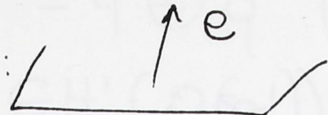
$$\text{Spin} = \{\pm 1\}$$

$$q(x) = \alpha x^2 \quad \alpha \in K^*$$

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

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



car symétrie:   $e^2 = 1$

(64)

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

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

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

Ex: Faire tout ceci explicitement...

$w_1$   $q$  forme quadratique  
 $w_2$   $n \geq 1$  rang  
 $\alpha \in H^1(K, O(q))$

$q_\alpha$  forme tordue par  $\alpha$ .

On veut calculer les invariants  $w_1, w_2$  de  $q_\alpha$  en fonction de  $\alpha$  et de ceux de  $q$ .

$$\begin{aligned} O(q) &\xrightarrow{\det} \{\pm 1\} \rightarrow 1 \\ \alpha \in H^1(K, O(q)) &\rightarrow H^1(K, \{\pm 1\}) = H^1(K) \\ &\xrightarrow{\quad} \delta_1^1(\alpha) \in H^1(K) \end{aligned}$$

D'autre part, suite exacte de gpes algébriques:

$$\begin{aligned} 1 &\rightarrow \{\pm 1\} \rightarrow \tilde{O}(q) \rightarrow O(q) \rightarrow 1 \\ \Delta: H^1(K, O(q)) &\rightarrow H^2(K) \quad \text{cobord.} \\ \alpha &\longmapsto \Delta\alpha := \delta_1^2(\alpha). \end{aligned}$$



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

(65)

$$\omega_2(q_\alpha) = \omega_2(q) + \omega_1(q) \cdot \delta'(\alpha) + \delta^2(\alpha)$$

Ou encore  $1 + \omega_1(q_\alpha) + \omega_2(q_\alpha) + \dots \equiv (1 + \omega_1(q) + \dots)(1 + \delta'(\alpha) + \dots)$   
mod termes de  $d \geq 3$

Si classe de cohomol. est ds  $SO(q)$ , la formule se simplifie... (et se trouve ds la littérature)

Corollaire Si  $q = \text{forme } \langle 1, \dots, 1 \rangle$   
 $\omega_1(q_\alpha) = \delta'(\alpha)$ ;  $\omega_2(q_\alpha) = \delta^2(\alpha)$ .

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

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

A vérifier  $\delta^2(\alpha) = \omega_1(q) \cdot \delta'(\alpha)$ .

$$q = ax^2 \quad \omega_1(q) = (a) \in H^1(K)$$

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

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

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

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

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

On a déjà trouvé une formule donnant le cobord de ce cas d'une telle action, à partir de la suite avec action triviale  $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$   
c'est celle qu'on veut!



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

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

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

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

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

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

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

Comme tjs, la 1<sup>ère</sup> est évidente. Pour la 2<sup>e</sup>

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



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

$$\begin{array}{ccc} \hat{O}(q') & \hookrightarrow & \hat{O}(q) \\ \hat{O}(q'') & \hookrightarrow & \end{array}$$

(mais pb du produit à cause de la commutation)

$$\text{si } g \in \hat{O} \rightarrow \hat{O} \xrightarrow{\det} (\pm 1)$$

$$\varepsilon(q) = \pm 1 \text{ image de } \pm 1$$

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

(se voit par exemple sur les symétries).

Calcul du cobord.

$$\delta^2(\alpha) \quad \alpha' \text{ repr. par } s \mapsto a'_s \in O(q') \quad s \in G_K$$

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

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

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

$$\alpha'' \quad a''_s, b''_s$$

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

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

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



$$\varepsilon(b''_s) \in \mathbb{Z}/2\mathbb{Z}$$

$$(s, t) \mapsto (-1)^{\varepsilon(b''_s) \varepsilon(b'_t)} b'_s \wedge b'_t (b''_s \wedge b''_t b_{st}^{-1}) \cdot b'_s$$

cobord de "  
de le centre

$$u \cdot v' \cdot v''$$

$$\text{avec } u = (-1)^{\varepsilon(b''_s) \varepsilon(b'_t)}$$

$$v' = b'_s \wedge b'_t b_{st}^{-1}$$

$$v'' = b''_s \wedge b''_t b_{st}^{-1}$$

$$\varepsilon(b''_s) = \varepsilon(a''_s) \text{ et } \varepsilon(b'_t) = \varepsilon(a'_t)$$

d'où la formule voulue.

Fin de la démonstration du thme sur la torsion

Récurrence 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  $(\varepsilon_i)$  base orthogonale de  $q$

$$(\pm 1)^m \hookrightarrow O(q).$$

$$O(1) \times \cdots \times O(1)$$

et  $H^1(\downarrow (\pm 1)^m) \rightarrow H^1(O(q))$  est surjectif

$$\alpha = (\alpha_1, \dots, \alpha_n) \in K^* / K^{*2}$$

$$q = \langle a_1, \dots, a_n \rangle$$

$$q_\alpha = \langle a_1 \alpha_1, \dots, a_n \alpha_n \rangle$$

on trouve donc tout !



octaves de Cayley  
 $e_0 = 1$

Remarque  $\nearrow G_2$   
 $(\pm 1)^3$

$e_i \equiv i \pmod 7$   
 $e_1 \mapsto \pm e_1$   
 $e_2 \mapsto \pm e_2$  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  $G_2$  st classées par les 3 formes de Pfister que l'on attrape avec le "petit" groupe).

On peut supposer  $\alpha = \alpha' \perp \alpha''$

d'où  $q_\alpha = q_{\alpha'} \oplus q_{\alpha''}$

$$\begin{aligned} w(q_\alpha) &= w(q_{\alpha'}) \cdot w(q_{\alpha''}) \\ &\equiv w(q') \cdot (1 + \delta'(\alpha') + \delta^2(\alpha')) \\ &\quad \cdot w(q'') \cdot (1 + \delta'(\alpha'') + \delta^2(\alpha'')) \pmod{\deg 3} \end{aligned}$$

$$w(q_\alpha) \equiv w(q) (1 + \delta'(\alpha) + \delta^2(\alpha)) \dots$$

d'où le thme.

### Remarques sur la caractéristique 2

On s'intéresse à q forme quadratique "non dégénérée" (donne quadrique lisse)

disc  $\neq 0$  (si disc bien défini).

En dim paire sur K algt clos  
impaire

$$\begin{aligned} &x_1 x_2 + \dots + x_{2m-1} x_{2m} \\ &x_0^2 + x_1 x_2 + \dots + x_{2m-1} x_{2m} \end{aligned}$$

On va attacher à ces formes des invariants

$n = 2m$   $O(q)$  lisse  
composante neutre  $SO(q)$

$$1 \rightarrow SO(q) \rightarrow O(q) \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0.$$

invariant de Dickson



(69)

$$\text{Si } \alpha \in H^1(O(q)) \longrightarrow \delta^1(\alpha) \in H^1(\mathbb{Z}/2\mathbb{Z}) = K/\mathfrak{o}K$$

$\mathfrak{o} x = x^2 + x \text{ en car } 2.$

définit l'invariant d'Arf de  $H^1$ , 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'est pas topo. étale ne donne pas ce qu'on veut~~

$$\alpha \in H^1(K, \text{SO}(q)) \longrightarrow \delta^2 \alpha \in H_{\text{fppf}}^2(\mu_2) \simeq \text{Br}_2(K)$$

En dim pair, les formes s'obtiennent comme

$$\alpha, x_1^2 + x_1 x_2 + \beta_1 x_2^2 + \alpha_3 x_3^2 + x_3 x_4 + \beta_3 x_4^2 + \dots$$

et  $\delta^2 \alpha = \sum [\alpha_i, \beta_i] \in \text{Br}_2(K)$  (à vérifier)

$$n = 2 \cdot m + 1$$

$O(q)$  pas lisse

$$1 \rightarrow \underset{\text{lisse}}{\text{SO}(q)} \rightarrow O(q) \xrightarrow{\det} \mu_2 \rightarrow 1.$$

en fait :  $O(q) = \mu_2 \times \text{SO}(q).$

$$\alpha \in H_{\text{fppf}}^1(O(q))$$

$$\det \alpha = \delta^1(\alpha) \in H_{\text{fppf}}^1(\mu_2) = K^*/K^{*2}$$

$$\delta^2(\alpha) \in \text{Br}_2(K).$$

car  $K \neq 2$

$$H^1(\text{SO}(q)) \xrightarrow{\alpha} H^1(O(q)) \text{ injective } (n \geq 1)$$

$$1 \rightarrow \text{SO} \rightarrow O \rightarrow \pm 1 \rightarrow 1$$

$$O(q)(K) \xrightarrow{\det} \{\pm 1\} \longrightarrow H^1(\text{SO}(q)) \xrightarrow{\alpha} H^1(O(q))$$



$O(q)(K) \rightarrow \{\pm 1\}$  surjective (reflections de déterminant -1). (70)

$\alpha^{-1}(1) = (1)$  "injectivité naïve" (ce n'est pas des groupes!).

Par torsion  $H^1(S O(q)) \xrightarrow{\text{injectif}} H^1(O(q)).$

$$H^1(K, \text{Spin}(q))$$



$$H^1(K, SO(q))$$

on note  $H^1(K, SO(q))_{\text{Spin}}$  l'image de cette flèche

Soit  $\alpha \in H^1(O(q))$ ,  $\alpha \in H^1(SO(q)) \Leftrightarrow \delta^1(\alpha) = 0.$

$$\alpha \in H^1(SO(q))_{\text{Spin}} \Leftrightarrow \begin{cases} \delta^1(\alpha) = 0 \\ \delta^2(\alpha) = 0 \end{cases}$$

$$w_i(q_\alpha) = w_i(q) \quad i=1,2$$



$\alpha$  est spinoriel.

On a une flèche canonique

$$H^1(K, SO(q))_{\text{Spin}} \xrightarrow{i (= i_3)} H^3(K).$$



$$Q_\alpha = q_\alpha \oplus (-q)$$

$$[Q_\alpha] \in W(K) \text{ (gpe de Witt de } K).$$

$W \supset I$  idéal d'augmentation  $\supset I^2$

$W/I \simeq \mathbb{Z}/2\mathbb{Z}$  ( $\leftarrow$  rg des formes mod 2).

$$I/I^2 \simeq H^1(K)$$



$$Q_2 \rightarrow 0 \text{ ds } I/I^2$$

$$I^2/I^3 \simeq H^2(K) \quad (\text{Mercurieu-Susler}).$$

La classe étant spinorielle, les  $w$  coïncident, d'où  $Q_2 \in I^3$ .

$$I^3/I^4 \simeq H^3(K) \quad (\text{Rost, M.S.}).$$

On ne se sert en fait  $I_{K^1}^3 \rightarrow H^3(K)$

D'où  $[Q_2] \rightarrow i_3(\alpha) \in H^3(K)$ .

Si  $i_3(\alpha) = 0$ , alors on peut définir  $i_4$  dans  $H^4(K)$ .

L'invariant  $i_3$ :

- Si on remplace  $q$  par  $\lambda q$ ,  $\lambda \in K^*$ , alors  $i_3(\alpha)$  ne change pas. En effet  $O(\lambda q), SO(\lambda q), H'(K, SO(\lambda q))_{\text{spin}}$  et resp.  $O(q), SO(q), H'(K, SO(q))_{\text{spin}}$

$$Q_\lambda = q_\lambda \oplus -q$$

$$\lambda Q_\lambda = \lambda q_\lambda \oplus -\lambda q$$

Si  $Q \in I^n$ ,  $\lambda Q \equiv Q \pmod{I^{n+1}}$

car  $\lambda Q - Q = (\lambda - 1)Q$  et  $\lambda - 1 \in I$ .

- $i_3(\alpha_1 \perp \alpha_2) = i_3(\alpha_1) + i_3(\alpha_2)$

$$\alpha_1 \in H'(K, SO(q_1, 1))_{\text{spin}}$$

$$\alpha_2 \in \text{---}$$

$$\alpha_1 + \alpha_2 \in H'(K, SO(q_1 + q_2))_{\text{spin}}$$

$$Q_{\alpha_1 \perp \alpha_2} = Q_{\alpha_1} \oplus Q_{\alpha_2}$$



$$i_3(\alpha_1 \otimes \alpha_2) = i_3(\alpha_1) \text{rang}(\alpha_2) + i_3(\alpha_2) \text{rang}(\alpha_1)$$

Démonstration:  $[q_{\alpha}] = [q] + \varepsilon \quad \varepsilon \in I^3$

$$i_3(\alpha) = \text{classe de } q_{\alpha} - q \text{ mod } I^4$$

$$q_{\alpha_1} \otimes q_{\alpha_2} = q_1 \otimes q_2 + q_1 \otimes \varepsilon_2 + q_2 \otimes \varepsilon_1 + \varepsilon_1 \varepsilon_2$$

on décompose  $q_1$  en somme:  $q_1 \otimes \varepsilon_2 = \underbrace{\varepsilon_2 + \dots + \varepsilon_2}_{\text{log } q_1 \text{ fois}} \text{ mod } I^4$

idem avec  $q_2$

$\varepsilon_1 \varepsilon_2 \in I^6$  donne 0 ds  $I^4$ , qfd.

On veut appliquer ceci à la cohomologie galoisienne des gpes non orthogonaux, par exemple exceptionnels

$$G \begin{cases} G_2 \\ F_4 \\ E_8 \end{cases} \quad \begin{array}{l} \text{pas d'automorph. externe} \\ \text{pas de centre.} \end{array}$$

$G$  sur  $K$  abs simple

$$G \simeq \text{Aut } G$$

- Les représentations irréductibles  $V$  de  $G$  sont "réalisables" sur  $K$ .  
Après extension, poids dominant  $\omega$   
 $V_{\omega} \text{ unéd } \longleftrightarrow \omega$

En fait  $V_{\omega}$  définissable sur  $K$ .

- Tous ces représent. st de type orthogonal.

On prend  $q_{\omega}$  une forme quadratique non dégénérée invariante par  $G$  sur  $V_{\omega}$ .  
d'où  $G \longrightarrow \text{SO}(q_{\omega})$  (car  $G$  connexe).



$G$  simple connexe, donc se relève

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \mathfrak{spin}(\mathcal{O}|_w) \\ & \searrow p_w & \downarrow \\ & & \mathfrak{so}(q_w) \end{array}$$

Si  $\alpha \in H^1(K, G)$ ,  $p_w(\alpha)$  est spinorielle, d'où un  $i_3(p_w \alpha)$   
Ne dépend pas de  $q_w$

D'où pour tout poids dominant  $w$  et tout  $\alpha \in H^1(K, G)$ , un elt  $i_w(\alpha) \in H^3(K)$

Exemple  $G = G_2$

Partons de la forme déployée

$$w = a\omega_1 + b\omega_2 \quad a, b \in \mathbb{N}$$

$\omega_1, \omega_2$  représentations de  $\mathfrak{d}_7$  et  $\mathfrak{l}_4$  respect.

(Octonions de trace 0) (rep. adjointe).

$$w = \omega_1 : H^1(K, G_2) \hookrightarrow H^3(K)$$

image formée des elts  
décomposables  $(a)(b)(c)$ ,  
 $(a), (b), (c) \in H^1(K)$ .

description par la 3-forme de Pfister

A démontrer:  $i_{a\omega_1 + b\omega_2}(\alpha) = \begin{cases} 0 \\ i_{\omega_1}(\alpha) \end{cases}$  dépend de  $a$  et  $b$

Ex:  $i_{\omega_2}(\alpha) \stackrel{?}{=} 0$ , ie forme de Killing

$$Kil_\alpha - Kil \in \mathbb{I}^4$$

$$\text{Avec } i_4(Kil_\alpha - Kil) \stackrel{??}{=} (-3) \cdot i(w)$$

$$Kil_\alpha = \langle 1, -3 \rangle \otimes \varphi_7$$

$$1 \oplus \varphi_7 = \varphi_8 \text{ (octonions)}$$



$$p \text{ qqa } i_p(x) \in H^3$$

$$i: R(G) \rightarrow H^3(K)$$

anneau des repr.

$$i(p_1 \oplus p_2) = i(p_1) + i(p_2)$$

$$i(p_1 \otimes p_2) = i(p_1) \cap p_2 + i(p_2) \cap p_1$$

$V_{w_1}, V_{w_2}$  engendrent  $R(G_2)$ , donc suffisait de connaître représent explicite .. (voir p. 111 bis)



18 février 1991

(75)

$G_2, F_4, E_8$

ss, simplement connexe

$$\text{Aut } G \cong G$$

Les repr. lin. de  $G$  sont "orthogonales"  
"définies sur  $K$ "

Principe:

$$\begin{array}{ccc} H/K & & \\ H & \xrightarrow{\rho} & GL_n = GL(V) \end{array}$$

$$\alpha \in H^1(K, H). \quad H_\alpha \xrightarrow{\rho_\alpha} GL(V_\alpha) \cong GL_n$$

s'il y a une f.q. invariante, non dégénérée  $q$   
 $q_\alpha$  est — " —.

$\rho$  irréductible, repr. de  $G$

$$H^1(K, G) \longrightarrow H^3(K) \quad i_3(\rho, \alpha)$$

$$\alpha \in H^1$$

$f: G \xrightarrow{\text{Spin}} SO$ , on choisit une f.q. invariante.

$$\text{On a: } H^1(K, G) \longrightarrow H^1(K, SO)_{\text{spin}} \xrightarrow{i_3} H^3(K).$$

Repr. irré'd. de  $G_2$  dépendent de 2 paramètres  $m, n$ .

Le foncteur  $i_3$  s'étend à toutes les  $\uparrow$   
représentations de  $G$ .

$$\underline{\text{car } K = 0}$$

Soit  $\rho$  une repr. lin. de  $V$ .

$$V \cong \bigoplus_{S \text{ irré'd}} S \otimes W_S$$

$W_S$  ev.  
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  $S$

$$q = \bigoplus q_S \otimes \phi_S$$

$\phi_S$  : forme quadratique non. de'g. sur  $W_S$   
ne compte que mod 2

On pose 
$$i_3(p, \alpha) = \sum_S \overline{\dim W_S} \cdot i_3(p_S, \alpha)$$

$\in H^3(K)$

A voir :

cler aussi le  $i_3$  associe' a'

$$H^1(K, G) \rightarrow H^1(K, \text{SO}(V, q))$$

$$\downarrow$$

$$H^3(K)$$

$$D_S \quad W(K)$$

$$n_S = \dim W_S$$

$$(q_S \otimes \phi_S)_\alpha - (q_S \otimes \phi_S) \equiv (q_S \otimes n_S)_\alpha - (q_S \otimes n_S) \pmod{I^4}$$

ou  $q_S \otimes n_S = q_S \oplus \dots \oplus q_S$ .



$$\underbrace{(q_s^2 - q_s)}_{\in \mathbb{I}^3} \otimes \underbrace{(\phi_s - h_s)}_{\in \mathbb{I}} \in \mathbb{I}^4$$

$$i_3(P_1 \oplus P_2) = i_3(P_1) + i_3(P_2)$$

$$i_3(P_1 \otimes P_2) = i_3(P_1) \text{rang}(P_2) + i_3(P_2) \text{rang}(P_1)$$

$\alpha$  fixe

$$i_3(\alpha): R(G) \rightarrow H^3(K).$$

détermine par ses valeurs sur des générateurs de  $R(G)$ , par exemple sur les représentations "fondamentales"  $P_1, \dots, P_\ell$  correspondant aux poids fondamentaux  $\omega_1, \dots, \omega_\ell$ .

Le cas de  $G_2$

$G = G_2$  déployé

$\alpha \in H^1(K, G_2)$ , d'où  $G_\alpha$  torseur

$C_\alpha$  algèbre d'octonions

forme norme  $\varphi_\alpha$  (3-forme de Pfister)

Inversement, toute 3-forme de Pfister définit un  $\alpha$  et un seul. On a :

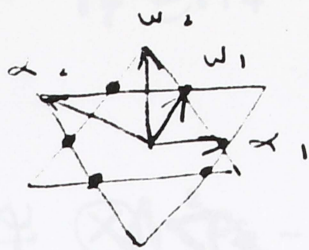
$$i_3(\varphi_\alpha) \in H^3(K).$$



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  $N = \Psi$ .

$$\Psi \simeq \underbrace{\langle 1, \alpha, \beta, \gamma, \alpha\beta, \alpha\gamma, \beta\gamma, \alpha\beta\gamma \rangle}_{\Psi_7}$$

$$\Psi \simeq \langle 1 \rangle \oplus \Psi_7$$

Forme quadratique: la norme  $N = \Psi$   
sur les éléments de trace 0, i.e.  $\Psi_7$ .

$$\Psi_7^\alpha - \Psi_7 = \Psi^\alpha - \Psi \quad (\Psi^\alpha = \langle 1 \rangle \oplus \Psi_7^\alpha)$$

Donc le  $i$  associé à cette repr. est celui que l'on connaissait déjà.

② dim 14

représentation adjointe: 2 fois 0, 12 racines.

Forme quadratique: forme de Killing.



$\text{Kill}^\alpha =$  forme de Killing de  $G_2$ .

Théorème :

$$\text{Kill}_\alpha \simeq \langle -1, -3 \rangle \otimes \varphi_7^\alpha.$$

On peut vérifier le cas déployé

$$\mathfrak{g} = \mathfrak{h} \oplus (\text{orthogonal})$$

$$X_\alpha, X_{-\alpha}$$

hyperbolique

$$\langle 1, 3 \rangle \simeq X^2 + XY + Y^2$$

$$\varphi_7 \simeq -1 \quad \text{dans} \quad W(K)$$

D'où le  $K$  dans le cas déployé.

[En caract. 3, cette forme est dégénérée.

La repr. de dim 14 est réductible  
en car. 3 : somme de 2 repr. de  
dim 7.]

$\lambda$  - structure : puissances extérieures.

$$q \mapsto \Lambda^i q. \quad \text{défini sur } Gr W.$$



$$\Lambda^2 P_7 \cong P_7 \oplus P_{14}$$

(dim 21 = 7 + 14)

$$P_{14} \longrightarrow \Lambda^2 P_7$$

$$V \longrightarrow SO(V)$$

$$\downarrow$$

$$\Lambda^2 V$$

$$\Lambda^2 P_7 \longrightarrow P_7$$

$x \wedge y \mapsto \pi(xy - yx)$  sur l'élé. de trace 0.  
en fait,  $\pi(xy)$  suffit.

On a  $\Lambda^2 P_7 \cong P_7 \oplus P_{14}$ . D'où :

$$\downarrow \quad \downarrow \text{Kill}$$

$$\psi_7$$

$$\Lambda^2 \psi_7 \cong \lambda \psi_7 + \mu \text{ Kill}$$

$$\lambda, \mu \in \mathbb{Q}^\times$$

indép. des choix

$$\psi_7 \cong \langle \alpha, \beta, \gamma, \dots \rangle$$

$$\Lambda^2 \psi_7 \cong \langle \alpha\beta, \alpha\gamma, \dots \rangle$$

21 produits

On constate que :

$$\Lambda^2 \psi_7 \cong \psi_7 \oplus \psi_7 \oplus \psi_7$$

Plus généralement :

Si  $\psi$  est une  $n$ -forme de Pfister, ~~unim~~ et si on pose :

$$\psi = \psi - \langle 1 \rangle, \text{ alors } \Lambda^2 \psi = (2^{n-1} - 1) \otimes \psi$$



$$\langle 1, 1, 1 \rangle \otimes \varphi_7 \simeq \lambda \varphi_7 + \mu \text{ Kill}$$

disc . Kill = 3 car vrai cas déployé

$$\text{disc } \varphi_7 = 1$$

On trouve  $\lambda = 3$  (à un carré près)

$$\langle 3 \rangle \varphi_7$$

Calcul de  $\mu = ?$

$$\gamma \cdot \text{Kill} \hookrightarrow \Lambda^2 \mathfrak{p}_7$$

"  $\mathcal{O}$  (7 variables)

Sur l'alg. de Lie d'un groupe orth.  
on a la forme trace  $\text{Tr}(xy)$ . Et:

$$\text{Kill} = 4 \cdot \text{forme trace}$$

(dans le cas déployé se voit sur les poids)

$$\text{Lie}(\underline{\text{SO}}) \simeq \Lambda^2 V \quad \text{On a } \begin{cases} \text{Trace} \\ \Lambda^2 \mathfrak{g} \end{cases}$$

$$\text{Trace} : -2 \times \Lambda^2 \mathfrak{g}$$

$$\text{Isom } \underline{\text{SO}} \simeq \Lambda^2 V \quad \text{donné par}$$

$V$  eq. avec forme bilin. sym.

$$\Lambda^2 V \rightarrow \underline{\text{SO}}(V)$$

$$v_1 \wedge v_2 \mapsto (x \mapsto B(v_1, x)v_2 - B(v_2, x)v_1)$$

Donc :  $\mu = -2$



D'où  $\langle -2 \rangle_{\text{Kill}} \oplus \langle 3 \rangle_{\Psi_7} \cong \langle 1, 1, 1 \rangle \otimes \Psi_7$

$\langle 1, 1, 1 \rangle = \langle 3, 2, 6 \rangle \cong \langle 3, 2, 6 \rangle \otimes \Psi_7$

$\text{Res } K \quad \text{Kill} \cong \langle -1, -3 \rangle \otimes \Psi_7$

$\text{Kill}^\alpha \cong \langle -1, -3 \rangle \otimes \Psi_7^\alpha$

$\text{Kill}^\alpha - \text{Kill} \cong \underbrace{\langle -1 \rangle}_{\in I} \otimes \underbrace{\langle 1, 3 \rangle}_{\in I} \otimes \underbrace{(\Psi_7^\alpha - \Psi_7)}_{\in I^3}$   
( $\Psi = \Psi_5$ )

C'est dans  $I^4$ . D'où :

$i_4(\alpha) \in H^4(K)$

$i_4(\alpha) = (-3) i_3(\alpha) \in H^4(K)$

$i_3(\alpha, p_4) = 0$

Conséquence

Pour toute représentation  $\varphi$  de  $G_2$ ,  
on a soit  $i_3(p, \alpha) = 0$ , soit  
 $i_3(p, \alpha) = i(\alpha) \in H^3(K)$

Si  $W = n_1 \omega_1 + n_2 \omega_2$ , comment  
(calculer explicitement  $i_3(p, \alpha)$  ? (Voir p. 111 bis)



Pour cela, il faut écrire  $V_w$  comme polynôme en  $p_1$  et  $p_2$ .

### Compléments sur les octonions et sur $G_2$ :

① Bourbaki, alg. III, dernier exercice (faute d'impression ! ) donne une formule montrant que les sommes de 16 carrés sont multiplicatives :

$\mathbb{C}$  alg. d'octonions

$$N(x) = x_0^2 + \alpha x_1^2 + \beta x_2^2 + \gamma x_3^2 + \alpha\beta x_4^2 + \dots$$

Posons :  $N(x) + \delta N(y) = \Phi$ .

C'est une forme à 16 variables, 4 - forme de Pfister.

Formule :

$$(N(x) + \delta N(y)) \cdot (N(z) + \delta N(t)) = N(x\bar{z} + \delta y\bar{t}) + \delta N(xt - xz, x^{-1})$$

$x, y, z, t \in \mathbb{C}$

$x^{-1} = \bar{x} / N(x)$ .

② A-t-on  $i_3(\alpha) = 0$  pour tout  $\alpha$  (et  $t \in \mathbb{P}$ ) (Probablement non.)

Pour  $F_4$ , l'invariant  $i_3(p, \alpha)$  est  $\neq 0$  pour certains  $p, \alpha$

(par exemple,  $K = \mathbb{R}$ ,  $p$  repr. adjointe) forme de Killing, signature

$i_3 \in H^3(\mathbb{R}) \simeq \mathbb{Z} / 2 \mathbb{Z}$ . Il y a 3 possibilités :

-5	2		compacte
4			déployée
-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  $T_r(xy)$  sur  $J$ , de rang 27

Algèbre de Jordan "réduite":

$$\exists e \in J, e^2 = e, e \neq 0, 1.$$

Les  $J$  réduites sont définies, au moyen d'une algèbre de Cayley  $O$ , 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  $3 \times 3$ , à coeff. de  $O$ , hermitiennes

$$\text{par. rap. } \begin{pmatrix} \gamma_1 & \gamma_2 & 0 \\ 0 & \gamma_2 & \gamma_3 \end{pmatrix} = \Gamma \quad (A\Gamma = \Gamma^t A)$$

$$\overline{J} = \begin{pmatrix} x_1 & c_3 & c_2 \\ \lambda_3 \overline{c_3} & x_2 & c_1 \\ \lambda_2 \overline{c_2} & \lambda_1 \overline{c_1} & x_3 \end{pmatrix}$$

où  $x_i \in K, c_i \in \mathbb{C}$

et  $\lambda_1 = \gamma_3/\gamma_2, \lambda_2 = \gamma_3/\gamma_1, \lambda_3 = \gamma_2/\gamma_1$

$$H^1(K, F_4)_{\text{red}} \subset H^1(K, F_4)$$

15  
classes de  $J$   
(réduites)



$J$  détermine l'algèbre d'octonions  $O$

3 - forme de Pfister  $q_8$

5 - forme de Pfister  $q_{32} = q_8 \otimes q_4$ , ou

$$q_4 = \langle 1, \gamma_1^{-1} \gamma_2, \gamma_2^{-1} \gamma_3, \gamma_3^{-1} \gamma_1 \rangle.$$

$J$  est déterminé à isom. près par

$q_8, q_{32}$  que l'on peut se donner

arbitrairement.

En effet,  $q_8$  et  $q_{32} \iff$  forme trace de  $J$

(Springer)

Conj. de Milnor  $\Rightarrow$  les alg. de Jordan  
réduites sont définies par

$$\begin{cases} x_3 \in H^3(K) \\ x_5 \in H^5(K) \end{cases} \quad \text{avec les conditions}$$

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.

$x_3 \neq 0, x_5 = 0$

$x_3 \neq 0, x_5 \neq 0$

(exerice...)

Ce sont les 3 cas de tout à l'heure



La forme trace est  $Q_J = 2(x_1^2 + x_2^2 + x_3^2) + \gamma_1^{-1} \gamma_2 N(c_3)$   
 $+ \dots + \gamma_2^{-1} \gamma_3 N(c_2).$

i.e.  $Q_J = \langle 2, 2, 2 \rangle \oplus \langle \gamma_1^{-1} \gamma_2, \gamma_2^{-1} \gamma_3, \gamma_3^{-1} \gamma_2 \rangle \otimes N.$

La connaissance de  $Q_J$  détermine à la fois la 3-forme de Pfister  $N$  et la 5-forme de Pfister  $N \otimes \langle 1, \gamma_1^{-1} \gamma_2 \rangle.$

On a  $N \in I^3$ ,  $\gamma N \in I^3$ ,  $\gamma N \equiv N \pmod{I^4}$ .

$$Q_J - \langle 2, 2, 2 \rangle \equiv N \pmod{I^4}.$$

Or, si  $(N, N')$  sont des 3-formes de Pfister, on a  
 $N \equiv N' \pmod{I^4} \Rightarrow N \cong N'.$

$$\text{5-forme} = Q_J - \langle 2, 2, 2 \rangle \oplus N.$$

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  $N \cong N'.$

$$N = \langle 1 \rangle \oplus \varphi_7, \quad N' = \langle 1 \rangle \oplus \varphi_7'$$

$\varphi_7 \cong \varphi_7'.$  On choisit  $\alpha \neq 0$  tel que  $-\alpha$  est représenté par  $\varphi_7$  et  $\varphi_7'.$



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  $K_2 = K \oplus Ke_1$  et  $K_2' = K \oplus Ke_1'$ .

Sur  $K_2^\perp$  on a  $\varphi_6 = \varphi - \langle 1, \alpha \rangle$  et de même  $\varphi_6'$ .

Par Witt:  $\varphi_6 \cong \varphi_6'$

Il existe <sup>donc</sup>  $(-\beta \neq 0)$  représenté par  $\varphi_6, \varphi_6'$ .

D'où  $\left\{ \begin{array}{l} e_2 \in C, \\ e_2' \in C' \end{array} \right.$  —————  $\begin{array}{l} e_2 \perp (1, e_1), \quad e_2^2 = \beta \\ e_2'^2 = \beta. \end{array}$

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 <sup>de  $K_4$</sup>  (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

Dans  $K_4^\perp$ , on choisit  $e_3 \in K_4^\perp$ ,  $e_3^2 = \gamma$ ,  
et  $e_3' \in K_4'^\perp$ ,  $e_3'^2 = \gamma$ .

On a  $C = K_4 \oplus K_4 \cdot e_3$

$C' = K_4' \oplus K_4' \cdot e_3'$

On trouve l'alg. d'oct. sur  $\alpha, \beta, \gamma$ .



Formules de produit:

$$c, d \in K_4 \quad e_3^2 = \delta$$

$$(a + be_3)(c + de_3) = ac + \delta \bar{d}b + (da - b\bar{c})e_3$$

(Autre façon (Tit) -

$V$  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 vecteurs de longueur 1, soit  $e, e', e''$ . On identifie  $V, V', V''$

(formes isom.), Loi de produit des oct.

$SO_3$  opère sur  $V, V', V''$

$$(x, y) \mapsto xy$$

$$C \cong \mathcal{O}_3 \text{ oct.}$$

$$(g \in \text{Spin } C$$

Re tour aux généralités sur les f. q.

théorèmes d'injectivité du  $H^1$

① Thm de Witt:  $q = q' \oplus q''$

$$\mathcal{O}(q') \hookrightarrow \mathcal{O}(q)$$

donc  $H^1(K, \mathcal{O}(q')) \hookrightarrow H^1(K, \mathcal{O}(q))$



(2)

Pfister

$$q = q' \otimes q''$$

(89)

$$O(q') \longrightarrow O(q)$$

$$x \longmapsto x \otimes 1$$

Th S: rang  $q''$  est impair, l'application

$$H^1(K, O(q')) \longrightarrow H^1(K, O(q))$$

est injective

(3)

Th (Springer)

Si  $K'/K$  est une ext. de degre' impair,  
alors la flèche naturelle

$$H^1(K, O(q)) \longrightarrow H^1(K', O(q)) \text{ est } \underline{\text{injective}}$$

||

$$H^1(K, O(q)) \longrightarrow H^1(K, R_{K'/K} O(q))$$

(2)  $\Rightarrow$  (3)

(D'abord, énoncés en termes de f.q.)

$K'/K$  extension. f.q.  $/K' \rightarrow$  f.q.  $/K$ . 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.  $\psi = x^2$  sur  $K'$ ,  $n = [K' : K]$

$\psi_\lambda$  forme :  $x \in K' \mapsto \lambda(x^2) = q_\lambda(x)$  ( $n$  variables).

$$\psi = \sum_{i=1}^r \alpha_i x_i^2, \quad \alpha_i \in K^*$$

$$\psi_\lambda = \sum \alpha_i \lambda(x_i^2) = \langle \alpha_1, \dots, \alpha_r \rangle \otimes q_\lambda$$

$$\psi_\lambda \equiv \psi \otimes q_\lambda.$$

Autre façon de voir :

$$O(q) \rightarrow R_{K'/K} O(q) \rightarrow O(q \otimes q_\lambda).$$

$$O(q), \text{ repr. } \rho$$

Condition générale sur  $\rho$  pour obtenir  
injectivité au niveau des  $H^1$ ? On ne sait pas...



car  $K \neq 2$ ① Théorème de simplification de Witt

$$H^1(K, O(q)) \rightarrow H^1(K, O(q+q'))$$

est injectif② (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

$$\parallel$$

$$H^1(K, R_{K/K} O(q))$$

②  $\Rightarrow$  ③ faitDémonstration de ②Il suffit de montrer que  $q \mapsto q \otimes q'$  définit  
une injection

$$W_K \rightarrow W_K$$

②  $\Leftrightarrow$   $(q')$  dans  $W_K$  est non diviseur de  
 $q'$  est de rang impair  $(\Rightarrow) q' \notin I$ 

$$W_K / I \cong \mathbb{Z}/2\mathbb{Z} \quad (\text{rang})$$

Lemme:  $\cap I^n = 0$  dans  $W_K$ 

Supposons que non. Alors il y aurait une

f. q. Q anisotrope de rang  $\geq 1$ , t. q. $(Q) \in I^n$  pour tout  $n$ .



Impossible si  $\text{rang}(Q) < 2^n$ . (92)  
 $q'$  est inversible mod tout  $I^n$ .

On voudrait avoir un critère, et a-t-on donc

$$\gamma: O(q) \rightarrow O(Q)$$

critère pour l'injectivité sur le  $H^1$ ?

Par exemple, puissances extérieures?

① On peut supposer  $q'$  de rang 1.

$$q' = \langle a \rangle, \quad a \in K^*.$$

Il suffit de démontrer que le noyau est 0.

$G_1 \subset G_2$  groupes algébriques

$$\text{Ker: } H^1(K, G_1) \rightarrow H^1(K, G_2) = ?$$

$$\begin{aligned} 1 \rightarrow H^0(G_1) \rightarrow H^0(G_2) \rightarrow \underbrace{H^0(G_2/G_1)}_X \rightarrow \\ \rightarrow H^1(G_1) \rightarrow H^1(G_2) \end{aligned}$$

Le noyau est donc

$X(K)/G_2(K)$  : ensemble des orbites de  $G_2(K)$  dans  $X(K)$ .



Injectivité'  $\Leftrightarrow G_2(K)$  opère transitivement  
sur les points rationnels de  
l'espace homogène  $X = G_2/G_1$ .

Ici  $X = O(\overbrace{q+q'}^q) / O(q)$

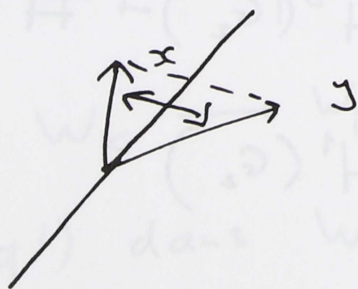
$$O_{n+1}'' / O_n$$

|||

Sphère des  $x \in K^{n+1}$  avec  $Q(x) = \alpha$ .

Quadrique affine. On est donc ramené à  
prouver l'énoncé classique suivant:

- (1') (Witt) Si:  $x, y$  sont deux vecteurs  
tels que  $Q(x) = Q(y) \quad (\neq 0)$   
alors il existe  $s \in O(Q)$ , rat./K,  
qui transforme  $x$  en  $y$ .



réflexion par rapport à  $x-y$  si

$x-y$  anisotrope. Si  $x+y$  non isotrope,

réflexion par rapport à  $x+y$ .

$x-y$ ,  $x+y$  tous les deux isotropes  
est impossible (sinon  $x \cdot x = 0$ ).



(2) et (3) :

$$O_n \hookrightarrow O_{nm} \quad n \text{ impair de } SO_{nm}(K)$$

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 Scharlau

$\lambda: K' \rightarrow K$  forme linéaire non nulle  
 $n = [K': K] \quad \lambda \mapsto q_\lambda$  de rang  $n$   
 $q_\lambda(x) = \lambda(x^2)$ .

$$W_K \xrightarrow{i} W_K, \quad \lambda \mapsto W_\lambda$$

$$\lambda \circ i(d) = q \otimes q_\lambda$$

Il existe des choix de  $\lambda$  qui sont  
tels que  $(q_\lambda) \cong \langle 1 \rangle$  dans  $W_K$ .

Choix de  $\lambda$  :

Supposons d'abord que  $K'$  soit une extension monogène de  $K$ . Soit  $t \in K'$  tel que  $K' = K(t)$   
 $K'$  base  $1, t, \dots, t^{n-1}$ .

$$\lambda(1) = 1 \quad \lambda(t^i) = 0, \quad 1 \leq i \leq n-1.$$

Lemme -  $q_\lambda \cong \langle 1 \rangle \oplus \frac{n-1}{2}$  forme hyperbolique

$$K' = K \oplus V, \quad V = Kt \oplus \dots \oplus Kt^{n-1}$$

$$q_\lambda(x, y) = \lambda(x \cdot y)$$

$$q_\lambda = \langle 1 \rangle \oplus q_{\lambda, V}$$

$$V \text{ contient } W = Kt \oplus \dots \oplus Kt^{\frac{n-1}{2}}$$

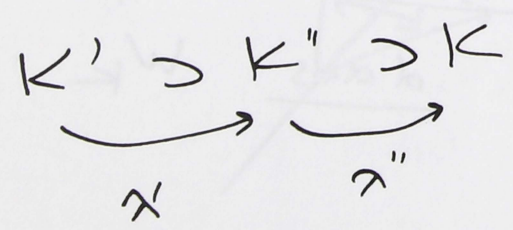
$$W \cdot W \subset V, \quad \lambda(w \cdot w) = 0$$

donc  $W$  est totalement isotrope de

dimension  $\frac{n-1}{2} \Rightarrow q_{\lambda, V}$  est hyperbolique.

D'où le lemme: on a bien  $q_\lambda \cong \langle 1 \rangle$  dans  $W_K$ .

Cas général: récurrence sur le degré de  $K$



$$\lambda = \lambda'' \circ \lambda'$$

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 :

$$q \text{ anisotrope sur } K \Rightarrow q \text{ anisotrope sur } K'.$$

(96)

Entraîne l'énoncé précédent.

Vrai en caract  $\neq$  aussi, avec la même démonstration.

Démonstration :

On peut supposer  $K'/K$  monogène,

$$K' = K[t]/(p(t)) \quad \begin{array}{l} p \text{ unitaire,} \\ p \text{ irréductible} \\ p \text{ de degré } n \end{array}$$

Récurrence sur  $n$ .

$$x = (x_1, \dots, x_N) \quad N \text{ variables.}$$

$$q(x'_1, \dots, x'_N) = 0 \quad \begin{array}{l} x'_i \in K' \text{ non} \\ \text{tous nuls.} \end{array}$$

$$x'_i = a_i(t) \quad d^0 a_i \leq n-1, \quad a_i \text{ sans facteur commun}$$

$$q(a_1(t), \dots, a_N(t)) \equiv 0 \pmod{p(t)}$$

$Q(t)$  de degré ?

Soit  $r$  le maximum des degrés des  $a_i$ .

$$a_i = \alpha_i t^r + \dots + \dots \quad \text{avec } \alpha_i \text{ non tous nuls.}$$

$$\begin{aligned}
 Q &= q(\alpha_1 t^r + \dots, \alpha_2 t^r + \dots, \dots, \alpha_N t^r + \dots) \\
 &= t^{2r} q(\alpha_1, \dots, \alpha_N) + \text{polynôme de degré} \\
 &\quad \text{à plus } 2r-1
 \end{aligned}$$

$q$  est anisotrope :  $q(\alpha_1, \dots, \alpha_N) \neq 0$ .

Donc degré de  $Q = 2r \leq 2n-2$

$$\begin{aligned}
 Q &= p Q' & \deg Q' &= 2r - h \\
 & & &\leq n-2 \\
 & & &\text{impair}
 \end{aligned}$$

Soit  $p'$  un facteur irréductible de degré impair de  $Q'$ .

$$Q \equiv 0 \pmod{p'}$$

$a_i(t)$  ne sont pas tous 0 mod  $p'$ .

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  $q_2 \Leftrightarrow q_1 \oplus (-q_2)$   
 contient  $r_2$  fois la  
 forme  $h = \langle 1, -1 \rangle$

$\Rightarrow$

$$q_1 = q_2 \oplus q_3$$

$$q_1 \oplus (-q_2) = q_2 \oplus (-q_2) \oplus q_3$$

$$\langle a \rangle \oplus \langle -a \rangle \cong \langle 1, -1 \rangle.$$

$$\cong r_2 h \oplus q_3$$

$\Leftarrow$

$$q_1 \oplus -q_2 = r_2 h \oplus q_3$$

$$= q_2 \oplus (-q_2) \oplus q_3$$

$\Rightarrow q_1 \cong q_2 \oplus q_3$  par Witt.

On est donc ramené à prouver que  
 si  $q$  contient  $n$  fois  $h$  sur  $K'$ ,  
 $q$  contient  $n$  fois  $h$  sur  $K$ .

$$Q = Q_{\text{anis}} + x h \quad \begin{matrix} x \geq n \\ x \geq n \end{matrix} \quad \begin{matrix} /K \\ /K \end{matrix}$$

(2)  $q$  forme quadratique /  $K$

Si  $q$  est une  $n$ -forme de Pfister sur  $K$   
alors — " — sur  $K$

$$\text{rang } q = 2^n = N$$

$q$   $n$ -forme de Pfister  $\Leftrightarrow$   $q$  est hyperbolique  
 ou  $q$  anis., et

il existe  $z_1, \dots, z_N$   
 $\in K(x, y)$

telles que

$$q(x) q(y) = q(z).$$

ou bien  $q$  est hyperbolique /  $K'$

donc sur  $K$

ou bien des  $z'_i \in K'(x, y)$  existent avec

$$q(x) q(y) = q(z').$$

$q$  représente  $q(x) q(y)$  sur  $K'(x, y) = K' \otimes_K K(x, y)$   
 de degré impair sur  $K(x, y)$



$q(x)q(y) \in K(x,y)$  est représentée

sur  $K'(x,y)$ , donc sur  $K(x,y)$

$$m = 1, 2, 3, \dots$$

$q$   $m$ -forme de Hilbert  $\Leftrightarrow q$  représentée  
invariants de  $q$

$H^i(K) \rightarrow H^i(K')$  injectif.

dans  $H^1, H^2, \dots$

$H^{m-1}$  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  $K' \sim$  diagonale

$H^m(K) \rightarrow H^m(K')$  injectif

(a)  $k_n^M K \rightarrow k_n^M K'$  injectif ?

oui : Bass-Tate, Kato  
(trace)  $\downarrow$  LN 342, p. 379, corollary

(b)

$$I_K^m / I_K^{m+1} \rightarrow I_{K'}^m / I_{K'}^{m+1}$$

injectif

Où: car le transfert  $I_{K'}^m \rightarrow I_K^m$

voir au th 2 lignes du haut de la p. 465

(J.K.) (Arason)  $\rightarrow$  Cohomologische Invarianten Quadratischer Formen, J. of Algebra 36 (1975), p. 448-491, p. 464, Satz 3.3.

Formes trace ; cas des algèbres centrales simples.

car  $K \neq 2$

$A$  algèbre simple centrale sur  $K$   
de rang  $n^2$

$$[A] \in Br(K)$$

$Tr_d$  = trace réduite de  $A$

$$q_A(x) = Tr_d(x^2)$$

forme bilinéaire correspondante ( $= \frac{1}{2}$  associé)  
est  $Tr_d(xy)$

cas déployé :  $A = M_n(K)$

$$Tr_d(x) = Tr(x) \quad x \in M_n(K), \quad x = (x_{ij})$$

$$Tr(x^2) = \sum x_{ii}^2 + 2 \sum_{i < j} x_{ij} x_{ji} \quad \text{Donc :}$$

$$q_A^{dec} = \underbrace{\langle 1, \dots, 1 \rangle}_n + \frac{n(n-1)}{2} h \quad h = \langle 1, -1 \rangle.$$



On va comparer  $q_A$  et  $q_A^{\text{dec.}}$ .

1<sup>er</sup> cas :  $n$  impair

Alors  $q_A \cong q_A^{\text{dec.}}$

En effet, il existe  $K'/K$  de degré impair qui décompose  $A$ .

Donc (\*) est vraie sur  $K' \Rightarrow$  vraie sur  $K$   
(grâce au théorème de Springer). Voici une application :

Thm (Wedderburn): car  $K \neq 3$

Si  $n=3$ ,  $A$  est une algèbre cyclique.

$[A] \in \text{Br}_3(K)$  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  $K \neq 2, 3$

A monter: il existe  $\alpha \in A$  avec

$$\alpha^3 \in K^* \text{ et } \text{Trd}(\alpha) = 0, \text{Trd}(\alpha^2) = 0.$$

pol. caract.  $t^3 - x$

Soit  $V$  espace vec. 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  $\mu_3$ ,  $A \supset K(\alpha) = K(\sqrt[3]{x})$

Si  $\mu_3 \notin K$ , posons  $L = K(\mu_3)$ .

On a une involution  $z \mapsto \bar{z}$  de  $L$   
opère sur la cohomologie de  $L$ .

On dispose d'un  $x \in K^*$ , non cube, tel que  
 $K(\sqrt[3]{x}) \subset A$ , d'où  $L(\sqrt[3]{x}) \subset A_L$ .

Donc, dans  $H^2(L, \mu_3)$ ,  $[A] = x \cdot y$   
avec  $y \in H^1(L, \mathbb{Z}/3\mathbb{Z})$ .

$$H^1(K, \mathbb{Z}/3\mathbb{Z})$$

(resp.  $\mu_3$ )  $\downarrow$  points fixes de l'involution  
agissant sur:

$$H^1(L, \mathbb{Z}/3\mathbb{Z}),$$

$$[\text{resp. } H^1(L, \mu_3)];$$

même chose pour :  $H^2(L, \mu_3)$ .



On écrit  $y = y^+ \oplus y^-$ , avec

$y^+$  invariant

$y^-$  anti-invariant.

$$[A] = x y^+ + x y^-, \quad (\text{invariant}) \quad [A] = [A^+]$$

$$x = x^+$$

donc:  $[A] = x y^+$   
 $y^+ \in H^1(K, \mathbb{Z}/3\mathbb{Z})$ , et l'on a  
 $[A] = x y^+$ , cqfd.

En fait, pour  $p$  premier et  $A$  algèbre  
centrale simple de rang  $p^2$ ,  $A$  est  
cyclique  $\Leftrightarrow A^*$  contient  $a$ ,  $a \in K$ ,  
 $\alpha p \in K$

autrement dit,  $A \supset K(\sqrt[p]{x})$   
 $x \in K^*$ .

Remarque —

$p=3$   $a^3 \in K^*$ ,  $a \notin K$

$x \mapsto axa^{-1}$  automorphisme de  $A$   
d'ordre 3.

Suffisant de ~~trouver~~ ~~prover~~ un sous-corps  
 $L$  commutatif maximal de  $A$ ,  
stable par  $\sigma$ , mais pas fixe par  $\sigma$ .

$PGL(A)$  groupe alg. plusieurs tores maximaux  
stables, ??

car 2 :

à résoudre  $\text{Tr } a = 0$  ,  $\text{Tr } a^2 = (\text{Tr } a)^2 = 0$   
 sol. après ext. de degré impair

→ solution.

car 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

$$w_1(q_A) = w_1(q_A^{\text{dec}}) = n_2(-1) \in H^1(K)$$

$$q_A^{\text{dec}} = n \langle 1 \rangle \oplus \dots \oplus n_2 h \quad \text{où } h = \langle 1, -1 \rangle$$

$$\text{et } n_2 = \frac{n(n-1)}{2}.$$

### Théorème

$$w_2(q_A) = w_2(q_A^{\text{dec}}) + \frac{n}{2} [A].$$

$$[A] \in \text{Br}_n(K) \quad \text{et} \quad n[A] = 0, \text{ d'où}$$

$$\frac{n}{2} [A] \in \text{Br}_2(K).$$

$$A = (A^{\text{dec}})_\alpha, \quad \alpha \in H^1(K, \text{PGL}_n)$$

$$A^{\text{dec}} = M_n$$



$$\mathrm{PGL}_n = \mathrm{Aut}(A^{\mathrm{dec}})$$

$A^{\mathrm{dec}}$  est un espace vect. muni de la  
forme quadratique  $q_A^{\mathrm{dec}} = (\mathrm{Tr}(xy))$

Tout automorphisme de  $A^{\mathrm{dec}}$  respecte  $q_A^{\mathrm{dec}}$

$$\begin{array}{ccc} \mathrm{PGL}_n & \xrightarrow{\varphi} & \mathrm{O}(q_A^{\mathrm{dec}}) \\ \text{"} & & \\ \mathrm{Aut}(A^{\mathrm{dec}}) & & \end{array} \quad (n^2 \text{ var.})$$

$$H^1(K, \mathrm{PGL}_n) \xrightarrow{\gamma} H^1(K, \mathrm{O}(q_A^{\mathrm{dec}}))$$

( $\gamma = H^1(\varphi)$ )

Foncteur algèbre simple centrale  $\rightarrow$  espace quadr.

$q_A$  est la torsion de  $q_A^{\mathrm{dec}}$  par

$$\gamma\alpha \in H^1(K, \mathrm{O}(q^{\mathrm{dec}}))$$

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

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

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

Par convexité, l'image de  $\mathrm{PGL}_n$  ds  $\mathrm{O}(q^{\mathrm{dec}})$   
est contenue dans  $\mathrm{SO}(q^{\mathrm{dec}}) \Rightarrow \delta^1 = 0$ .

$$\begin{array}{c}
 1 \\
 \downarrow \\
 \pm 1 \\
 \downarrow \\
 \text{Spin}(q) \\
 \downarrow \\
 \text{SO}(q) \\
 \downarrow \\
 1
 \end{array}$$

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

$$w_2(q_\beta) = w_2(q) + \delta^2(\beta)$$

$$\beta \in H^1(K, \text{SO}(q))$$

$$\begin{array}{ccc}
 M_n & \xrightarrow{\gamma} & M_2 \\
 \downarrow & & \downarrow \\
 \text{SL}_n & \xrightarrow{\gamma} & \text{Spin}(q_A^{\text{dec}}) \\
 \downarrow & & \downarrow \\
 \text{PGL}_n & \xrightarrow{\varphi} & \text{SO}(q_A^{\text{dec}})
 \end{array}$$

car  $\text{SL}_n$  est simplement connexe.

$$\gamma(\zeta) = \begin{cases} 1 \\ \zeta^{n/2} \end{cases}$$

$$\gamma(\zeta) = \zeta^{n/2}$$

Lemme:

Donc  $\gamma$  est surjectif.

admettons le lemme pour le moment.



$$\alpha \in H^1(K, PGL_n) \rightarrow H^2(K, \mu_n) = Br_n(K)$$

$$\downarrow \sim$$

$$\downarrow$$

$$H^1(K, SO) \longrightarrow H^2(K, \mu_2)$$

L'image de  $\alpha$  ds  $Br_n(K)$  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  $n$  est divisible par 2, il faut prendre la cohomologie plate.]

Il reste à prouver le lemme :

si  $\gamma$  n'est pas surjectif,  $\gamma = 1$ ,

la flèche  $SL_n \rightarrow Spin$  se

factoriserait en  $PGL_n \rightarrow Spin$

$\gamma$  se relèverait en  $\tilde{\gamma}$ .

$$PGL_n \xrightarrow{\quad} Spin_{n^2} \downarrow$$

$$PGL_n \rightarrow SO_{n^2}$$

à voir que non.

Technique connue en th. des groupes alg.  
pour voir si une repr. se relève aux spinous.

$G$  réductif connexe,  $\rho$  représentation  
orthogonale de  $G$ .

On choisit un tore maximal  $T$ .

Poids de  $\rho$  (écrits additivement)

poids 0 multiplicité quelconque  
paires  $(w_i, -w_i)_{i \in I}$  avec même multiplicité,  $w_i \neq 0$ .

On forme alors  $\sum_{i \in I} w_i$ ; le résultat est :

$$\sum w_i \equiv 0 \pmod{2} \text{ dans } X(T)$$

(les  $w_i$  sont répétées suivant leurs multiplicités)



$\rho$  spinorielle

Remarquons que  $-\frac{w_1}{2} + \dots + \frac{w_n}{2} = \frac{w_1}{2} + \dots + \frac{w_n}{2} - w_1$

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'ens.

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  $PGL_n$  agissant sur  $M_n$

par autom. int. sont 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)



De 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.

$w = (n-1)e_1 + \dots \quad w \not\equiv 0 \pmod{2}$

car  $n$  est pair.

Rappel sur  $G_2$ 

car 0  $i : H^1(K, G_2) \hookrightarrow H^3(K, \mathbb{Z}/2\mathbb{Z})$

$$\omega = n_1 \omega_1 + n_2 \omega_2$$

repr.  $f_\omega : H^1(K, G_2) \rightarrow H^1(K, SO_\omega)_{\text{spin}} \rightarrow H^3(K)$

$$i_\omega : H^1(K, G_2) \rightarrow H^3(K)$$

$$i_\omega = \begin{cases} 0 & \text{ou} \\ i & \end{cases}$$

$$\omega = 0 \quad \text{unité ou } \omega = \omega_2 \quad (\dim 14)$$

$$\omega = \omega_1 \quad (\text{repr. de dim } 7)$$

$$\omega \equiv \omega' \pmod{8} \Rightarrow i_\omega = i_{\omega'}$$

Pour  $n_1, n_2 \leq 8$ , on détermine les valeurs de  $i_\omega$   
(voir tableau, page suivante)

retour à  $\text{Tr}(x^2)$

$A$  algèbre simple centrale,  $n^2 = [A:K]$

$$q_A(x) = \text{Trd}(x^2) \quad \text{rang } n^2$$

$$n \text{ impair} \quad q_A \simeq q_A^{\text{dec}}$$

$$n \text{ pair} \quad w_1(q_A) = w_1(q_A^{\text{dec}})$$

$$w_2(q_A) = w_2(q_A^{\text{dec}}) + \frac{n}{2} [A]$$

$$q_A - q_A^{\text{dec}} \in I_K^2$$

$$I_K = \text{idéal max. de } W_K$$

$$\text{cl}(q_A - q_A^{\text{dec}}) \in I_K^2 / I_K^3 \cong \text{Br}_2(K)$$

$$\frac{n}{2} [A].$$



Tableau donnant les valeurs de  
l'invariant  $i_\omega$  pour  $G_2$

On écrit  $\omega = n_1 \omega_1 + n_2 \omega_2$  où  $\omega_1, \omega_2$  sont les 2 poids fondamentaux ( $\omega_1 \rightarrow$  repr. de dim. 7 ;  $\omega_2 \rightarrow$  rep. adjointe).  
L'invariant  $i_\omega$  est  $\varepsilon_\omega i$ , avec  $\varepsilon_\omega = 0$  ou  $\pm 1$ ,  $i$  étant l'invariant naturel ( $= i_{\omega_1}$ ).

La valeur de  $\varepsilon_\omega$  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 <sub>1</sub>	0 <sub>14</sub>	1 <sub>77</sub>	1 <sub>273</sub>	0	0	0	0
1	1 <sub>7</sub>	0 <sub>64</sub>	0 <sub>296</sub>	0	1	0	0	0
2	1 <sub>27</sub>	0 <sub>189</sub>	0	1	0	0	0	0
3	0 <sub>77</sub>	0	0	0	0	0	0	0
4	0 <sub>182</sub>	0	0	1	0	0	1	0
5	0	0	1	0	0	0	1	0
6	0	0	0	1	1	0	0	0
7	0	0	0	0	0	0	0	0

(En indice : dimension de la rep., en caract. 0)

Noter  $i_\omega = 0$  si  $n_2 \equiv 1, 5, 7 \pmod{8}$

Cas particulier  $n=4$

$$[A] \in Br_4(K), \quad \frac{n}{2}[A] = 0 : [A] \in Br_2(K)$$

Alors  $A = A_1 \otimes A_2$ ,  $A_1$  alg. quat.

$$A_\lambda = (a_\lambda, b_\lambda) \quad \lambda = 1, 2.$$

$$q_A - q_A^{\text{dec}} \in \mathbb{I}_K^3. \quad \text{Image ds } \mathbb{I}_K^3 / \mathbb{I}_K^4 \cong H^3(K)$$

$$q_A = q_{A_1} \otimes q_{A_2}.$$

Soit  $(a, b)$  un corps de quaternions.

Forme norme  $N$ :

$$x = x_0 + x_1 i + x_2 j + x_3 k, \quad k = ij$$

$$Nx = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$$

$$N(a, b) = \langle 1, -a, -b, ab \rangle.$$

Forme trace:

$$x^2 = (x_0^2 + ax_1^2 + bx_2^2 - abx_3^2) + \dots$$

$$q_{(a, b)} = 2 \langle 1, a, b, -ab \rangle$$

$$q_A = \langle 1, a_1, b_1, -a_1 b_1 \rangle \otimes \langle 1, a_2, b_2, -a_2 b_2 \rangle$$

comparer à la norme:

$$N_{ab} + \left\langle \frac{1}{2} \right\rangle q_{(a, b)} = \langle 1 \rangle + \langle 1 \rangle = 2$$

dans  $W_K$

$$q_A = (2 - N_1) \otimes (2 - N_2) \quad N_1 = N_{a_1, b_1}, \quad N_2 = N_{a_2, b_2}.$$



$$N_2 = N_{a_2}, b_2. \quad q_A^{\text{dec}} = 4.$$

$$\begin{aligned} q_A - q_A^{\text{dec}} &= 4 - 2(N_1 + N_2) + N_1 N_2 - 4 \\ &= -2(N_1 + N_2) + N_1 N_2. \end{aligned}$$

$$2 \in I_K, \quad N_2 \in I_K^2, \quad \text{donc}$$

$$q_A - q_A^{\text{dec}} \in I_K^3.$$

classe dans  $I_K^3 / I_K^4$  ?

$$2 \longrightarrow I_K / I_K^2 = H^1(K)$$

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

$$2 \longrightarrow (-1) \in H^1(K).$$

$$q_A - q_A^{\text{dec}} \longrightarrow (-1)(x_1 + x_2) = (-1)[A] \in H^3(K).$$

$$x_2 = [A_1] \in H^2(K)$$

Que se passe-t-il si  $-1$  est un carré ds  $K$  ?

$$(-1) = 0 \text{ ds } H^1(K).$$

$$2 = \langle 1 \rangle - \langle -1 \rangle = 0 \quad (\text{car } \langle 1 \rangle = \langle -1 \rangle)$$

$$2 = 0 \text{ dans } W_K.$$

$$q_A - q_A^{\text{dec}} = N_1 \cdot N_2 \in I_K^4$$

$$\text{classe de } q_A - q_A^{\text{dec}} \text{ dans } I_K^4 / I_K^5$$

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 dépend pas de la décomposition

$$x = x_1 + x_2.$$

Suggère chercher une opération cohomologique:

$$-1 = \square$$

Théorème: (Sous l'hypothèse que  $-1$  est un carré dans  $K$ .)

Il existe une unique application

$$\varphi: H^2(K) \rightarrow H^4(K)$$

telle que:

$$(a) \quad \varphi(x+y) = \varphi(x) + \varphi(y) + xy$$

$$(b) \quad \varphi(x) = 0 \quad \text{si} \quad x = a \cdot b, \quad \text{avec} \quad a, b \in H^1(K)$$

Si on admet ce thm,  $\varphi(x) = x_1 x_2$  est l'application ci-dessus.

Cartan a étudié la notion de

Puissance divisée dans les algèbres.  $\left(\frac{x^n}{n!}\right)$

$C$  anneau commutatif,  $J$  idéal

$$\gamma_i: J \rightarrow C \quad i = 0, 1, 2, \dots$$

$$\gamma_0(x) = 1, \quad \gamma_1(x) = x, \quad \dots, \quad \gamma_n(x+y) = \sum_{i+j=n} \gamma_i(x) \gamma_j(y)$$

(d'autres propr.)

$$\gamma_n(xy) = x^n \gamma_n(y) \quad \begin{matrix} y \in J \\ x \in C \end{matrix}$$



(dans Cartan:  $C$  commutatif gradué,  
 $J$  : idéal des élé de degré  $\geq 1$ )

$$\Rightarrow n! \gamma_n(x) = x^n.$$

Exemple:  $k$  anneau commutatif  
 $M$   $k$ -module

$$C = \bigwedge^{\text{pair}} M$$

Il y a sur  $C$  (sur les élé  $> 0$ )

des  $\gamma_i$  uniques tels que

$$\gamma_i(x_1 \wedge \dots \wedge x_{2i}) = 0 \quad i \geq 2, n \geq 1.$$

(voir G. Papy, Thèse  
~~pas dans la lit.~~ On le fait pour modules  
libres - sém. Cartan, puis on écrit le  
module comme quotient)

$M$  libre de rang  $2n$ ,  $u \in \bigwedge^{2n} M$

$$Pf(u) = \frac{u^n}{n!} \in \bigwedge^{2n} M$$

$$= \gamma_n(u)$$

$K$ -théorie de Milnor  $k^M(K)$

algèbre graduée sur  $\mathbb{F}_2$

générateurs  $(x)$ ,  $x \in K^* / K^{*2} = H^1(K)$

relations  $(x)(1-x) = 0$ ,  $x \neq 0, 1$   $x \in K$ .

$$\Rightarrow (x)(-x) = 0$$

comme  $-1 = \text{carre}$ ,  $(x)^2 = 0$

(116)

$$k^M(K) = \Lambda H^1(K)/J$$

$J$  engendré par  
les  $(x)(1-x)$ .

(par certains élém.  
décomposables).

Lemme:

Si  $J \subset \Lambda M$  est un idéal engendré par  
des éléments décomposables de degré 2, alors  
les  $\gamma_i$  de  $\Lambda M$  définissent par passage  
au quotient des puissances divisées sur  $C = (\Lambda M/J)^{\text{pair}}$ ,  
(définies sur élé de degré pair),  $\gamma_i(x) = 0 \quad i \geq 2$   
 $x$  décomposable.

$$x \in \Lambda^{2n} M, \quad y \in \Lambda^{2n} M, \quad y \in J$$

$$\text{à vérifier : } \gamma_i(x+y) = \gamma_i(x) \text{ mod } J$$

récurrence.

Montre l'existence de puissances divisées sur  
 $k^M(K)$  lorsque  $-1 = \square$ .

En particulier,

$$\begin{array}{ccc} \gamma_i : k_2^M(K) & \longrightarrow & k_{2i}^M(K) \\ & & \downarrow \\ & & H^{2i}(K) \end{array}$$



Conclusion : on a

(117)

$$\gamma_i : H^2(K) \rightarrow H^{2i}(K)$$

$$X = \sum_{\lambda \in L} x_\lambda \quad \begin{array}{l} x_\lambda \text{ décomposables} \\ L \text{ ordonné totalement} \end{array}$$

$$\gamma_i(X) = \sum_{\lambda_1 < \dots < \lambda_i} x_{\lambda_1} \dots x_{\lambda_i}$$

$i=2$  donne  $\gamma_2 = \varphi$  de tout à l'heure.

Autre façon d'obtenir  $\varphi$  : utiliser les puissances extérieures,  $\wedge$ -structure de  $W_K$ .

A algèbre centrale simple,  $n=3$

A est cyclique,  $[A] = x \cdot y$   $x \in H^1(K, \mu_3)$   
(car  $K \neq \mathbb{F}_3$ )  $y \in H^1(K, \mathbb{Z}/3\mathbb{Z})$

Remarque : ces algèbres sont classées par  
 $H^1(K, PGL_3)$  s/g naturel de type  $(3,3)$   
(donc Heisenberg ds  $GL_3$ )

$$\begin{pmatrix} 1 & \rho & \rho^2 \\ & \rho & \rho^2 \\ & & \rho^3 \end{pmatrix} \quad \rho^3 = 1 \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \sigma$$

$$\rho \sigma = * \sigma \rho$$

$\uparrow$  homothétie

On note :

$$\Phi = \mu_3 \rtimes \mathbb{Z}/3\mathbb{Z} \hookrightarrow PGL_3, \text{ sous-groupe d'ordre 9}$$

$$H^1(K, \phi) \longrightarrow H^1(K, \mathrm{PGL}_3)$$

surjective

"

$$H^1(K, \mu_3) \times H^1(K, \mathbb{Z}/3\mathbb{Z}) \ni (x, y)$$

à vérifier : l'image de  $x, y$  dans

$$H^1(K, \mathrm{PGL}_3) \text{ est } x \cdot y$$

$\cap$

$$H^2(K, \mu_3)$$

(ou  $-x \cdot y$  ??)

(Analogie orthogonale :

$$(\pm 1) \times \dots \times (\pm 1) \longrightarrow O_n$$

et surjectif sur  $H^2$ .)

$n=5$  : on ne sait pas si l'alg. est toujours cyclique.

Formes traces des corps et des algèbres  
étales.

$\mathrm{car} \neq 2$

Algèbres étales sur  $K$

$E$  algèbre commutative de dim finie  $n$  sur  $K$

(a)  $E$  isom. à un produit  $\prod E_i$

$E_i$  corps, ext. sép. de  $K$



$$\sum n_i = n, \text{ ou } n_i = [E_i : K].$$

(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 bien connu (Bourbaki)

$K_s$  clôture séparable de  $K$

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

$$E \xrightarrow{\varphi} K_s \quad K\text{-homomorphisme}$$

$$\Phi_E = \text{Hom}_{K\text{-alg}}(E, K_s), \quad |\Phi_E| = n$$

action naturelle de  $G_K$

$$s \in G_K, \quad \varphi \in \Phi_E \quad s \cdot \varphi \in \Phi_E$$

action continue à gauche.

Équivalence de catégories ("th de Galois")

$K$ -algèbres étales et ensembles finis munis

d'une action continue de  $G_K$ .

( $G_K$ -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<sup>er</sup> cas:  $\sum m_i \equiv 0 \pmod{2}$

Alors  $q_E$  contient la forme  $\langle 1, \dots, 1 \rangle$  h fois.

i.e.  $q_E \cong \underbrace{\langle 1, \dots, 1 \rangle}_h + q$ ,  $q$  de rang  $n-h$ .

2<sup>ème</sup> 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  $\Phi_E$ ,  
ens. à  $n$  éléments.

À isom. près,  $E$  est déterminée par

$$\varphi_E : G_K \rightarrow S_n.$$

Classes d'algèbres étales de degré  $n$   
correspondent aux représentations galoisiennes

$$\varphi_E : G_K \rightarrow S_n \quad \bar{\alpha} \text{ conj. près.}$$

$G_E$  = image de  $G_K$  dans  $\text{Aut}(\Phi_E) \simeq S_n$   
groupe de Galois associé à  $E$



1<sup>ère</sup> étape

Démontrer le thm quand l'image de  $G_K$  est  
un 2 - groupe

2<sup>ème</sup> étape

Ramener le cas général à celui-ci.

On choisit un 2 - groupe de Sylow de  $G_E$ ,  
et on prend son image réciproque ds  $G_K$ ,  
c'est  $G_{K'}$ , avec  $[K':K]$  impair.

Par le thm de Springer, il suffit de  
montrer la 1<sup>ère</sup> étape.

1° Les orbites de  $G_K$  ds  $\phi_E$  sont  
d'ordres des puissances de 2.

Il existe une décomposition de  $\phi_E$   
en sous-ensembles d'ordres  $2^{m_1}, \dots, 2^{m_r}$  stables  
par  $G_K$ .

Décomposition de  $\phi_E$  en ss/ens. d'ordres puissances  
de 2, stables par  $G_K$ .

On la choisit avec nombre minimum de  
facteurs

$$n = 2^{a_1} + \dots + 2^{a_k} \quad \text{d'c. de } n$$

correspondant.

les  $a_i$  sont distincts.

Donc les  $a_i = m_i$  à permutation près.

$$E = E_1 \times \dots \times E_h \quad \deg E_i \text{ est } 2^{m_i}.$$

$$q_E = \sum q_{E_i} = \bigoplus q_{E_i}.$$

$$T_{V_{E_i}}(1^2) = 2^{m_i}.$$

$$q_{E_i} \cong \langle 2^{m_i} \rangle \oplus g_i \quad \text{rang } g_i = 2^{m_i} - 1$$

$$q_E \cong \langle 2^{m_1}, 2^{m_2}, \dots, 2^{m_h} \rangle \oplus g$$

$$m_i \text{ pair} \Rightarrow \langle 2^{m_i} \rangle = \langle 1 \rangle$$

$$m_i \text{ impair} \Rightarrow \langle 2^{m_i} \rangle = \langle 2 \rangle.$$

De plus  $\langle 2, 2 \rangle = \langle 1, 1 \rangle$ . D'où le résultat.

$$d(q_E) = \text{disc}(E) \in K^\times / K^{\times 2} = H^1(K).$$

$$h = 1, 2, 3$$

$$\underline{h=2} \quad E = K(\sqrt{a}) \quad , \quad q_E = \langle 2 \rangle \oplus g$$

$$q_E = \langle 2 \rangle \oplus \langle 2d \rangle$$

$$\underline{h=3}$$

$$q_E \cong \langle 1, 2, 2d \rangle$$

$d = \text{disc}$

Pour aller plus loin, il faut connaître l'invariant de Witt.



$$\underline{w_1, w_2 (qE)}$$

$$\varphi_E : G_K \rightarrow S_n \quad \text{d'hi: à conjugaison près.}$$

$$H^i(S_n, \mathbb{Z}/2\mathbb{Z})$$

$$i = 1, 2$$

$$H^1(S_n) \simeq \begin{cases} 0 & n=1 \\ \mathbb{Z}/2\mathbb{Z} & n \geq 2 \end{cases}$$

$$n=1 \\ n \geq 2$$

$$S_n \xrightarrow{\text{sgn}} \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$$

$$\varepsilon_n = \text{élément non nul de } H^1(S_n)$$

$$H^2(S_n) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & n=2,3 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & n \geq 4 \end{cases}$$

(Schur)

$$\varepsilon_n^2 \in H^2(S_n)$$

$H^2_0$

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

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

$$\downarrow$$

$$\downarrow$$

$$X$$

$$\longrightarrow$$

$$C_4$$

$$\downarrow$$

$$\downarrow$$

$$S_n$$

$$\longrightarrow$$

$$\{\pm 1\}$$

une transposition devient d'ordre 4

$$\text{Res}_H \varepsilon_n^2 \neq 0$$

$$H = \{(1), (12)\}$$

Autre élément de  $H^2(S_n)$ :

$$\tilde{S}_n \longrightarrow \tilde{O}_n(\mathbb{C})$$

$$\downarrow \qquad \qquad \downarrow$$

$$S_n \longrightarrow O_n(\mathbb{C})$$

$$s_n \in H^2(S_n)$$

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.

$$S_n = 0 \quad \text{si} \quad n \leq 3.$$

$$S_n, \varepsilon_n^2 \text{ ind.} \quad n \geq 4$$

$$H^2(S_n) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & n=2, 3 \\ & \text{base } \varepsilon_n^2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & n \geq 4 \\ & \text{base } \varepsilon_n^2, s_n \end{cases}$$

Autre définition :

$$H^i(\mathcal{B}O_n(\mathbb{R})) \longrightarrow H^i(S_n)$$

$$H^*(\mathcal{B}O_n(\mathbb{R})) = \mathbb{F}_2[w_1, \dots, w_n]$$

$$w_i \mapsto \varepsilon_i$$

$$w_i \mapsto s_i$$



$$S_n \rightarrow O_n(\mathbb{R})$$

$$BS_n \rightarrow BO_n(\mathbb{R})$$

125

Démonstration de Schur :

$S_n$  : présentation "à la Coxeter"  
de type  $A_{n-1}$   $\circ - \circ - \circ \dots$

$n-1$  éléments d'ordre 2,

$$\sigma_1, \dots, \sigma_{n-1}$$

$$\left\{ \begin{array}{l} \sigma_1 = (12) \quad \sigma_2 = (23) \quad \dots \quad \sigma_{n-1} = (n-1, n) \\ \sigma_i^2 = 1, \quad \sigma_i \sigma_j = \sigma_j \sigma_i \quad \text{si } |i-j| \geq 2 \\ (\sigma_i \sigma_j)^3 = 1 \quad (\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j) \\ |i-j| = 1. \end{array} \right.$$

$\tilde{S}_n$  peut être présentée par des  $\tilde{\sigma}_i$ ,  $-1 \in \text{centre}$

avec  $\tilde{\sigma}_i^2 = 1$

$$\tilde{\sigma}_i \tilde{\sigma}_j = -\tilde{\sigma}_j \tilde{\sigma}_i \quad |i-j| \geq 2$$

$$(\tilde{\sigma}_i \tilde{\sigma}_j)^3 = 1 \quad \text{si } |i-j| = 1.$$

Pour vérifier que  $\tilde{S}_n$  existe, il  
utilise les spineurs.

DS  $\tilde{O}_n$ , on peut relever les symétries  $S_x$   
ou  $q(x)$  est un  
carré.

Théorème (CMH, 1984).

$$(a) \quad w_1(q_E) = \varphi_E^*(\varepsilon_n)$$

$$(b) \quad w_2(q_E) = \varphi_E^*(s_n) + (2)w_1(q_E)$$

$$d = \text{disc } E$$

$$w_1(q_E) = d$$

$$w_2(q_E) = \varphi_E^*(s_n) + (2)(d).$$

Démonstration par torsion galoisienne

$$E^{\text{dec}} = K \times \dots \times K \quad n \text{ fois}$$

$$q_E^{\text{dec}} = \langle 1, \dots, 1 \rangle \quad \text{forme unitaire}$$

$$\varphi: G_K \rightarrow S_n = \text{Aut}(E^{\text{dec}})$$

$\psi$  est un 1-cocycle à valeurs ds

$$\text{Aut}(E^{\text{dec}}).$$

$E$  est  $E^{\text{dec}}$  torsu par  $\varphi$ .

$$E = (E^{\text{dec}})_{\varphi}.$$

$$q_E = (q_E^{\text{dec}})_{\varphi}$$

$$\varphi: G_K \rightarrow S_n \subset O_n(K)$$

groupe orthogonal pour  
la forme unitaire



$$2 q_E = (2 q_E^{dec}) \varphi$$

(127)

$$\begin{array}{ccc} S_n & \hookrightarrow & O_n \\ (ij) & \mapsto & \text{réflexion p.r. } \bar{a} \quad e_i - e_j \\ & & q(e_i - e_j) = 2 \end{array}$$

$$2 q(e_i - e_j) = 4 \quad \text{correct!}$$

$$\tilde{S}_n \hookrightarrow \tilde{O}(2 q_E^{dec}) = \tilde{\Sigma}(K)$$

$$\downarrow \quad \quad \pi \downarrow \quad \quad \downarrow$$

$$S_n \subset O(2 q_E^{dec}) = \Sigma(K)$$

$S_n$  contenu dans l'image de  $\tilde{\Sigma}(K)$ .

Lemme:

$$\text{Soit } 1 \rightarrow A \rightarrow \tilde{\Sigma} \rightarrow \Sigma \rightarrow 1$$

une suite exacte de groupes algébriques

$$A \subset \text{centre } \tilde{\Sigma}, \quad A \text{ fini, et } A(\bar{K}) = A(K)$$

$$\text{Soit } \tilde{G} \text{ un s/g fini de } \tilde{\Sigma}(K)$$

$$\text{contenant } A = A(K) \text{ et soit } G$$

$$\text{son image dans } \Sigma(K)$$

$$\tilde{G} \subset \tilde{\Sigma}$$

$$\downarrow \quad \quad \downarrow$$

$$G \subset \Sigma$$

Alors, les 2 éléments suivants de  $H^2(G_K, A)$  coïncident:

- ①  $\varphi$  est un 1-cocycle sur  $G_K$ ,  
 $\bar{a}$  valeurs dans  $\Sigma$ ; 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 définit  $e \in H^2(G, A)$   
 $\varphi^* e \in H^2(G_K, A)$

On a:  $\varphi^* e = \Delta[\varphi]$ .

Rappelons la définition de  $\Delta$ .

$\tilde{a}_s$  relève  $a_s \in \Sigma(K_s)$

$$\Delta(a_s)(s, t) \mapsto \tilde{a}_s (\tilde{a}_{st})^{-1} \tilde{a}_t$$

ici  $a_s \tilde{a}_s$  sont rationnels sur  $K$ .

donc  $= \tilde{a}_s \tilde{a}_t (\tilde{a}_{st})^{-1}$ .



$E$  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  $n$

$$d = \text{disc}(q_E) = \text{disc}(E)$$

$$w_1(q_E) = (d) \in H^1(K).$$

$E \leadsto \varphi_E: G_K = \text{Gal}(K_S/K) \rightarrow S_n$   
défini à conjugaison près

$$s_n \in H^2(S_n, \mathbb{Z}/2\mathbb{Z})$$

$$\varphi_E^*(s_n) \in H^2(G_K, \mathbb{Z}/2\mathbb{Z}) = H^2(K).$$

Théorème  $w_2(q_E) = \varphi_E^*(s_n) + (2)(d)$

$(q)_\alpha = q_E$ ,  $q = q^{\text{dec}}$ , forme associée à  $K \times \dots \times K$

$$\alpha: G_K \xrightarrow{\varphi_E} S_n \subset O_n(K)$$

$$w_2(2q_E) = ?$$

$$O(2q_E^{\text{dec}}) = O(\langle z, \dots, z \rangle) \leftarrow \tilde{O}(2q_E^{\text{dec}})$$

$$\sum_{\substack{V \\ S_n}} \longleftarrow \sum_{\substack{\tilde{V} \\ \tilde{S}_n}} \longleftarrow \sum_{S_n}$$

$$\alpha \in H^1(K, \Sigma)$$

$$1 \rightarrow C_2 \rightarrow \tilde{\Sigma} \rightarrow \Sigma \rightarrow 1$$

$$\Delta: H^1(K, \Sigma) \rightarrow H^2(K).$$

$$\text{On a : } \Delta(\alpha) = \varphi_E^*(s_n) \quad (\text{lemme})$$

$Q$  forme quadratique,  $\alpha \in H^1(K, O(Q))$

$$w_1(Q_\alpha) = w_1(Q) + \delta^1(\alpha)$$

$$w_2(Q_\alpha) = w_2(Q) + \delta^1(\alpha)w_1(Q) + \delta^2(\alpha)$$

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

$$Q = \sum q^{dec}. \quad w_1(Q_\alpha) = w_1(Q) + (d)$$

$$w_1(\sum q) = w_1(\langle z, \dots, z \rangle) + (d)$$

$$\text{d'où } w_1(q) = (d) \dots$$

$$w_2(\sum q) = w_2(\sum q^{dec}) + (d)w_1(\sum q^{dec}) + \varphi^*(s_n)$$

$$\text{Formules : } \begin{cases} w_1(\lambda q) = w_1(q) + n(\lambda) \\ w_2(\lambda q) = w_2(q) + n_1 w_1(q)(\lambda) + n_2(-1)(\lambda) \end{cases}$$

$$\text{où } n_1 = n-1, \quad n_2 = n(n-1)/2.$$

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

$$w_2(\langle \lambda \alpha_1, \dots, \lambda \alpha_n \rangle) = \sum_{i < j} (\alpha_i)(\alpha_j) + (\lambda)(\alpha_i) + (\lambda)(\alpha_j) + (-1)(\lambda)$$

$\lambda = 2$  donc :

$$w_2(\sum q) = w_2(q) + n_1(2)w_1(q)$$

$$w_2(q_E) + n_1(2)(d) = n(2)(d) + \varphi_E^*(s_n)$$

d'où la formule.

Bruno Kahn : formules pour les classes de Stiefel-Whitney supérieures, en fonction des  $\varphi_E^*(w_i(S_n))$



$$S_n \rightarrow O_n(\mathbb{R})$$

$$w_i(S_n) \in H^i(S_n, \mathbb{Z}/2\mathbb{Z})$$

$w_i(q_E)$  en fonction des  $\varphi_E^*(w_i(S_n))$  :

$$w = \sum w_i(q_E) = \varphi_E^*(w(S_n)) \cdot (1 + (2)(d))$$

Applications et cas particuliers :

Relèvement

$$\begin{array}{ccc} \tilde{\varphi} & \dashrightarrow & \tilde{S}_n \\ & & \downarrow \\ \varphi : G_K & \longrightarrow & S_n \end{array}$$

Condition de relèvement ?

$$\text{Exist. de } \tilde{\varphi} \quad (\Leftrightarrow) \quad \begin{array}{l} \varphi^*(S_n) = 0 \\ \text{"} \\ w_2(q_E) + (2)(d) \end{array}$$

n petit, 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<sup>ème</sup> degré.

Que signifie "résoudre une équation" ?

(problème d'histoire des maths).

Supposons  $\text{car}(K) \neq 2, 5$  (pas indispensable)  
 $A_5$  agit-il fidèlement sur une courbe de genre 0? (132)

Vrai sur un corps algébriquement clos

$$A_5 \hookrightarrow \text{PGL}_2(K), \quad K \text{ assez gros}$$

Si un tel plongement existe,  $\sqrt{5} \in K$ .

Si  $K \ni \sqrt{5}$ , il existe une courbe de genre 0  $Y$  sur laquelle  $A_5$  agit.

On obtient un revêtement ramifié en 3 pts  
 (moins en caract. 3)

$$Y \quad g=0$$

$$\downarrow A_5$$

$$X \cong \mathbb{P}^1$$

Une courbe de genre 0 a un invariant  
 $\in H^2(K)$ . Inv. de  $Y$  :  $(-1)(-1)$ .

( $\sqrt{5} \in K$ : choisissons  $s \in A_5$ , d'ordre 5

$$A_5 \rightarrow \text{PGL}_2(K)$$

$$\text{Tr}(s^2 / \det(s))$$

$$\frac{(1+w)^2}{w} = 2 + w + w^{-1} \Rightarrow a + b\sqrt{5}$$



$K$  quel conque.

(133)

$S$ :  $\sqrt{5} \notin K$ , on obtient

$Y$  source sur  $K(\sqrt{5})$  munie d'une action de  $S_5$  qui est  $A_5$  linéaire, et semi-linéaire en dehors de  $A_5$ .

$$\begin{array}{ccc} Y & & \\ \downarrow & & \\ \mathbb{P}_1 / K(\sqrt{5}) & Y/A_5 & K(\sqrt{5}) \\ \downarrow & & \downarrow \\ \mathbb{P}_1 & Y/S_5 & K \end{array}$$

$$Y_P \subset Y$$

$$\downarrow \quad \downarrow$$

$$P \in Y/S_5 = \mathbb{P}_1$$

$$P \in Y/S_5(K)$$

non ramifié

$$Y_P \quad S_5 \text{ - torsueur sur } K$$

$$\Leftrightarrow G_K \rightarrow S_5$$

$$\Leftrightarrow \text{algèbre étale de dim 5 sur } K$$

$$\Leftrightarrow \text{équation de 5<sup>ème</sup> degré} \\ (\bar{\alpha} \text{ equiv. pès}).$$

"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  $K(\sqrt{\alpha}, \sqrt{\beta})$ ,  $\alpha, \beta$   
convenables.

( $\alpha, \beta$  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  $\sum x_i = 0$ ).

$Y =$  variété des droites de la quadrique  $C$ .

Courbe à 2 composantes connexes de  
genre 0

$S_5$  agit en permutant par la  
signature les 2 composantes.

$C$  quadrique sur  $K$ .  $G_K$  agit sur  
l'ensemble des composantes.

( $q$  de rg 4, corps de def.  $K(\sqrt{\Delta(q)})$ )



$$\langle 1, \dots, 1 \rangle = \langle 5 \rangle + \langle 5, 1, 1, 1 \rangle$$

disc. 5

$$G_K \rightarrow \{\pm 1\} \text{ associée à } K(\sqrt{5}).$$

2°) Corps des fonctions de  $X$  (méthode modulaire).

D'abord sur  $\mathbb{Q}$ . Corps des fonctions  
modulaires de niveau 5 sur  $\mathbb{Q}(\zeta_5)$

$\zeta_5$  racine 5<sup>ème</sup> de 1, appelle'  $K_5$ .

Action de  $GL(2, \mathbb{F}_5) / \{\pm 1\}$ .

Invariants  $\mathbb{Q}(j)$

$$G_5 \left( \begin{array}{c} K_5 \\ | \\ \mathbb{Q}(\zeta_5, j) \\ | \\ \mathbb{Q}(j) \end{array} \right) \mathbb{F}_5^*$$

$$G_5 \xrightarrow{\det} \mathbb{F}_5^*.$$

$$\mathbb{F}_5^* / (\pm 1) \subset G_5$$

2 cli'

$k_5$  corps des invariants,

$$\begin{array}{c} k_5 \\ | \\ G_5(\mathbb{F}_5^* / (\pm 1)) \\ \mathbb{Q}_j \quad \parallel \\ \text{DCL / E 1-5} \end{array}$$

Donc on trouve

136

$$S_5 \left( \begin{array}{c} k_5 \\ | \quad A_5 \\ \mathbb{Q}(\sqrt{5})(j) \\ | \\ \mathbb{Q}(j) \end{array} \right)$$

calcul :  $k_5$  est de genre 0.

On a donc reconstitué la situation précédente.  
Les deux constructions sont isomorphes.

(Il faudrait ajouter  $\sum \sigma_i = 0, \sum \sigma_i^2 = 0$ ).

car  $K \neq 2, 5, |K| \geq$  assez grand

Théorème Soit  $E/K$  une algèbre étale  
de dim 5, avec  $(d) = (5)$ .

Les propriétés suivantes sont équivalentes:

- ①  $E$  est obtenable par la  
construction de Klein
- ②  $w_2(q_E) = (-1)(-1)$
- ③ Il existe  $x \in E, x \neq 0$ , avec  
 $\text{Tr } x = \text{Tr } x^2 = 0$
- ④ Il existe  $f(x) = x^5 + ax^2 + bx + c$   
tel que  $E \simeq K[x]/(f)$ .
- ⑤ La forme  $q_E \simeq \langle 5, 1, -1, 1, -1 \rangle$   
 $= \langle 5 \rangle + H$ .



Extensions quadratiques:

-  $\sqrt{5}d$  " irr. essentielle "

- choisir ext. quadr. forçant  $T_v x = 0 = T_v x^2$

à avoir un te'o  
" irr. accessoire "

Brumer a un que " irr. accen. " obrait donc  
par un élé' de  $Br_v$ .

$$E = K.1 \oplus H$$

$H$ : éléments de  $T_v 0$

$$q_E = \langle 5 \rangle \oplus q_E'$$

$$q_E' = q_E / H$$

$$\begin{cases} d(q_E') = 1 \\ q_E' \text{ de rang } 4 \end{cases}$$

Lemme: Si  $Q$  de rang 4,  $d(Q) = 1$

dans  $K^x / K^{x2}$ .

Les 3 propriétés <sup>suivantes</sup> sont équivalentes

(a)  $Q$  repr. 0

(b)  $w_2(Q) = (-1, -1)$

(c)  $Q \simeq \langle 1, -1, 1, -1 \rangle$ .

$$q_E = q_E' + \langle 5 \rangle$$

$$w_2(q_E) = w_2(q_E') + (1)(5) = w_2(q_E').$$

Supposons ⑤.  $q'_E$  est alors hyperbolique (138)

$$x \neq 0 \quad T_v x = 0 = T_v x^2 = 0$$

sont les points d'une quadrique déployée /  $k$

On veut un tel  $x$  avec  $K[x] = E$  tout entier.

Sur  $\overline{K}$ ,  $E \sim \overline{K} \times \dots \times \overline{K}$ .

On veut  $x$  tel que  $x_1, \dots, x_5$  distinctes.

quad. dépl.  $(q+1)^2$  points.

10 coniques.

Marche pour  $q > 9$ .

Il faut vérifier  $q = 3, 7, 9$

(sauf erreur, ne marche pas pour  $q = 9$ ,  
marche pour  $q = 3$ ).

①  $\Leftrightarrow$  ② etc.

De façon générale, lorsque  $Y$   
est un rev. gal. fini étale,  $\begin{matrix} Y \\ \downarrow^G \\ X \end{matrix}$

$G_K \xrightarrow{\varphi} G$  alg. gal.

A quelle condition  $\varphi$  provient-il d'un  
point rationnel de  $X$ ?

Recette la variété  $Y_\varphi$  (tordue de  $Y$   
par  $\varphi$ ) 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 prend  $Y$   
par  $\varphi$ . Pt rationnel ?

$Y^{dec}$  = variété des droites de la quadrique

$$T_v x = T_v x^2 = 0.$$

(moins points ramifiés)

$Y_\varphi$  = variété des droites de la quadrique

$$T_{v_E} x = T_{v_E} x^2 = 0.$$

Point rationnel dessus ?

critère (3).

---

On peut essayer d'aller plus loin: contrôle  
sur invariants supérieurs.

$E$  avec  $w_1(q_E) = 0$  d'ordre  $\varphi_E: G_K \rightarrow A_n$   
 $w_2(q_E) = 0$   $\varphi_E$  relevable dans  $\tilde{A}_n$

On a une forme quadratique  $q_E$  avec

$q_E$  et  $q_E^{dec} = \langle 1, \dots, 1 \rangle$  mêmes  $w_1, w_2$

$$q_E - q_E^{dec} \in I_K^3 \rightarrow H^3(K)$$

$$i_3(E) = \text{image de } q_E - \langle 1, \dots, 1 \rangle$$

(140)

dans  $H^3(K)$ .

calculer  $i_3(E)$  ?

Premier cas intéressant :  $n=6$ .

$$\varphi_E : G_K \rightarrow \tilde{A}_6$$

$H^i(\tilde{A}_6, \mathbb{Z}/2\mathbb{Z})$  : cohomology stable du  
2-groupe de Sylow.

$$S_2(A_6) = D_4$$

On trouve :  $H^1 = H^2 = 0$  pour  $\tilde{A}_6$

$$H^3(\tilde{A}_6, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$$

(vrai pour  $\tilde{A}_n$  ?)

(Nakaoka ~ 1950)

Soit  $u$  la classe non triviale de  $H^3(\tilde{A}_6)$

$$\varphi : G_K \rightarrow \tilde{A}_6$$

$$\varphi^* u \in H^3(K).$$

Est-ce que  $i_3(E) = \varphi^*(u)$  ?

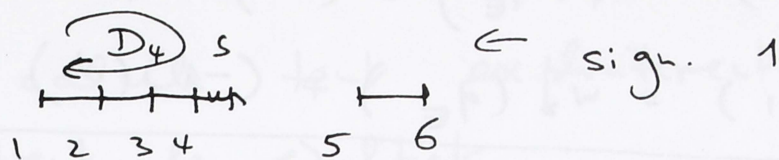
Vrai si  $\sqrt{2} \in K$  (mais en fait cet invariant est toujours 0 !).

Principe basé sur le théorème de Springer.



On peut supposer que  $\varphi(G_K) \subset S_2(A_6)$  (141)

$$\varphi_E(G_K) \subset S_2(A_6) = D_4$$



$D_4 \hookrightarrow S_4$ ,  $D_4 \hookrightarrow S_2$ , combinés  
pour sign. 1.

On peut calculer la forme quadratique  
grâce à ça.

Question liée :  $n=6$

$S_6$  a un automorphisme externe

$$\text{Out}(S_6) = \mathbb{Z}/2\mathbb{Z}$$

(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, génériquement, si

Comment comparer  $q_E$  et  $q_{E'}$  ?

$$\boxed{\begin{aligned} w_1(q_{E'}) &= w_1(q_E) = (d) \\ w_2(q_{E'}) &= w_2(q_E) + (-1)(d) \end{aligned}}$$

$H^i(S_6)$ ,  $i=1,2$  action de l'automorphisme externe

sur  $H^1(S_6) = \mathbb{Z}/2$  action est triviale

sur  $H^2(S_6)$  action non triviale

base  $\Sigma_6^2, S_6$

action de l'élément non trivial de  $\text{Out}(S_6)$

est

$$\Sigma_6^2 \mapsto \Sigma_6^2$$

$$S_6 \mapsto S_6 + \Sigma_6^2$$

$$(12) \mapsto (12)(34)(56).$$

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 les 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,  $G = SL_3(\mathbb{F}_2) = PSL_3(\mathbb{F}_2)$

Représentation naturelle  $G \xrightarrow{p} A_7$   
 $\xrightarrow{p'} A_7$   
 $Aut((2,2,2))$

action sur 7 points  $\rightarrow p$  et  $p'$   
 7 droites

D'où

$$\varphi: G_K \rightarrow G \begin{array}{l} \nearrow A_7 \\ \searrow A_7 \end{array}$$

d'où 2 algèbres ~~quadratiques~~ étale  
 de rang 7,  $E$  et  $E^\dagger$ .

Faible à voir que  $q_E$  et  $q_{E^\dagger}$  ont

le même  $w$ , ( $=0$ )

— " —

$w_2$

Théorème :

(144)

On a

$$\varphi_E \cong \langle 1 \rangle \oplus \varphi_6$$

$$\varphi_E \cong \langle 1 \rangle \oplus 2\varphi_6$$

on  $\varphi_6$  est de rang 6

$$\text{On a : } \varphi_E \cong \langle 1 \rangle \oplus \underbrace{\langle 1 \rangle \oplus \langle 2 \rangle \oplus \varphi_4}_{\varphi_6}$$

Ceci découle du thm sur  $A_6$ .

Par Springer, on peut supposer que

$$\varphi(G_K) \subset S_2(G) = D_4$$

$$\begin{array}{ccccc} D_4 & \hookrightarrow & A_6 & \hookrightarrow & A_7 & \text{fixant 1 pt} \\ & & \downarrow \text{a.v.} & & \nearrow & \\ & & A_6^{\text{ext}} & & & \end{array}$$

$$D_4 \rightarrow A_6 \xrightarrow{\text{ext}} A_6 \rightarrow A_7$$

$$E = K \times E_6, \quad E' = K \times E'_6$$

$$\varphi_E = \langle 1 \rangle \oplus \varphi_{E_6}$$

$$\varphi_{E'} = \langle 1 \rangle \oplus \varphi_{E'_6}$$

$$\Rightarrow \varphi_{E'_6} \cong 2\varphi_{E_6}.$$



18/3/91

145

Retour sur l'exemple quintique:

$|K|=q$  les coniques sont en fait non disjointes  
 corps  $\mathbb{F}_3, \mathbb{F}_7, \mathbb{F}_q$  E algèbre étale de dg 5 sur K  
 d'nc 5 (mod 5) est de la forme  
 $K[X] / X^5 + a_1 X^4 + \dots + a_5$   
 avec  $a_1 = a_2 = 0$ .

classe de conjugaison  $c \in S_5$

Quand 5 est un carré ( $q=9$ ),  $c$  doit être ds  $A_5$   
pas ( $q=3$  ou  $7$ ),  $c$  ds  $S_5 - A_5$

ds  $A_5$   $c = (1), (12)(34), (123), (12345)$

ds  $S_5 - A_5$   $c = (12), (123)(45), (1234)$

ie

$$E = \underbrace{\mathbb{F}_q \times \dots \times \mathbb{F}_q}_{5 \text{ fois}}, \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \mathbb{F}_q, \mathbb{F}_{q^3} \times \mathbb{F}_q \times \mathbb{F}_q, \mathbb{F}_q$$

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  $q=3$

$$F = \underbrace{(X^3 - X)}_{\substack{\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \\ (3 \text{ racines})}} \underbrace{(X^2 + 1)}_{\mathbb{F}_{q^2}} = X^5 - X$$

$$f = \underbrace{(X^3 - X + 1)}_{\substack{\text{irred de} \\ d^0 3}} \underbrace{(X^2 + 1)}_{\mathbb{F}_{q^2}} = X^5 + X^2 - X + 1$$

$$f = \underbrace{(X^4 + X - 1)}_{\text{irred de } d^0 4} X$$



# Algèbres à involution

146

$K$  car  $K \neq 2$

$A$   $K$ -algèbre associative, elt unité, de dimension finie, munie d'un anti-automorphisme involutif  $x \mapsto x^*$  (ou  $x^\top, x^\dagger, \dots$ )

$$\begin{cases} x \mapsto x^* \text{ est } K\text{-linéaire} \\ (xy)^* = y^* x^* \\ (x^*)^* = x \end{cases}$$

Structure  $\mathfrak{r} = \text{radical de } A$

$\mathfrak{r}$  est stable par  $x \mapsto x^*$

$$0 \rightarrow \mathfrak{r} \rightarrow A \rightarrow B \rightarrow 0$$

$B = A/\mathfrak{r}$  s. simple

$C = \text{centre de } B$  (stable par l'involution)

$$C = \prod_{\alpha \in \Sigma} K_\alpha \quad K_\alpha \text{ ext. finies de } K.$$

Cette décomposition est "stable par l'involution"  
l'involution opère sur  $\Sigma$ .

d'où une déc.

$$C = \prod_{\beta \text{ fixe}} K_\beta \times \prod_{\substack{\gamma \text{ et } \gamma^* \\ \text{échangés}}} (K_\gamma \times K_{\gamma^*})$$

L'algèbre  $B$  est aussi découpée en

$$B = \prod B_\beta \times \prod B_\gamma$$

$\gamma$  est  
de représ.  
" $\gamma^* \neq \gamma$ ."

centre de  $B_\beta$  est  $K_\beta$  un corps,  $B_\beta$  simple  
centre de  $B_\gamma$  est  $K_\gamma \times K_{\gamma^*}$  (échangés par involution)  
 $B_\gamma$  simple.



L'involution dans le 1<sup>er</sup> cas ( $B_\beta$ ) opère sur  $K_\beta$ .  
Dans le second cas, elle échange  $K_\beta$  et  $K_{\beta'}$ .  
sur  $K_\beta$  :  
action triviale ou par  $K_\beta / K_\beta^0$  quadratique.

Hypothèse présumée  $K$  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 st échangées par l'involution

① :  $x \mapsto x^*$  anti-automorphisme

Or  $x \mapsto {}^t x$  est involution

On sait que les automorphismes st intérieurs  $x \mapsto yxy$

Donc il existe  $y \in A^{**}$ , tq

$$x^* = y^+ x y^{-1}$$

$$x^{**} = y(y^+ x y^{-1})^+ y^{-1} = y^t y^{-1} x^t y y^{-1}$$

$$\text{donc } {}^t y y^{-1} = \lambda \in K^\times \quad {}^t y = \lambda y \text{ donc } \lambda = \pm 1$$

d'où 2 possibilités  $\lambda = 1$ ,  $y = {}^t y$  cas orthogonal  
 $\lambda = -1$ ,  $y = -{}^t y$  cas symplectique  
ceci n'est possible que si  $n$  pair

② Si on identifie le 1<sup>er</sup> morceau <sup>ops</sup> le second tel  
que  $(x, y) \mapsto ({}^r y, {}^t x)$ .



$K$  non alg<sup>r</sup> des

(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 induit. orthog ou sympl.

②  $L$  non fixé

$L_0$  sous corps fixé

$A \otimes_{L_0} L_s$  est du 2<sup>e</sup> type

③  $L \times L$

$A \simeq B \times B^o$   $B$  alg. simple centrale  
les deux facteurs étant échangés par  
l'involution

Cas séparables des

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  $PGln$ .

$n$  impair  
d'un scalaire

Toute similitude est produit  
et d'une tr orth.

$n$  pair  
 $n = 2m$

2 types

$\langle sx, sy \rangle = \lambda \langle x, y \rangle$   
 $\det(s) = \pm \lambda^m$

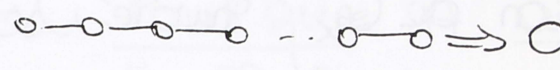


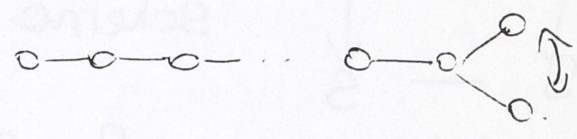
type I similitude  $\rightarrow \begin{cases} n \text{ impair} & \text{Aut} = O_n / \{\pm 1\} = SO_n \\ n \text{ pair} & \text{Aut}^\circ \text{ indice 2 de Aut} \end{cases}$


type symplect.  $\rightarrow \begin{cases} \text{Aut}^\circ = O_n / \{\pm 1\} \\ \text{Aut} = Sp_n / \{\pm 1\} \end{cases}$


type II  $\rightarrow \begin{cases} \text{Aut}^\circ \text{ indice 2} \\ \text{Aut}^\circ = PGln \end{cases}$

# Comparaison aux diagrammes de Dynkin (des groupes classiques)

type I  $n$  impair  $n \neq 1$   $B_{\frac{n-1}{2}}$    $\Rightarrow$  pas d'autom. externes. c'est connexe.

$n$  pair  $n \neq 4, 2, 8$   $D_{\frac{n}{2}}$  

type sympl.  $C_{n/2}$  

type 2 compos.  $n \neq 1, 2$   $A_{n-1}$  

$K$  A algèbre déployée simple.  
(comme algèbre associative).  
cas orthogonal : forme standard =  $\begin{cases} \text{hyperbol. si } n \text{ pair} \\ \text{hyperb sinon} \end{cases}$

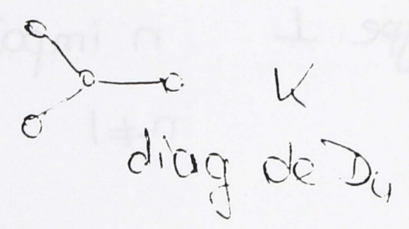
$A \rightarrow$  gpe simple (adjt) = comp neutre  
/ de Aut A  
G déployé.  
de l'un des types classiques.



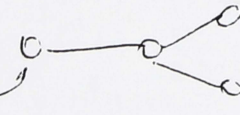
On a aussi un isomorphisme de  $\text{Aut } A \rightarrow \text{Aut } G$ .  
[Weil, OC, II] Les  $K$ -formes de  $A$  correspondent  
aux  $K$ -formes de  $G$ .

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 :



$G \quad S'$   
 $\downarrow \quad \downarrow$   
 $S \quad - \quad S$  schéma des schémas de Dynkin

trialitaire : les 3 sommets ext. st permutés.  
sinon 1 sommet fixe  et on a  
alg. à involution.

Voir pourquoi on s'intéresse aux algèbres à  
involution - elles fournissent toutes les  
formes des groupes classiques !



Théorème (Albert)

Soit  $A$  une algèbre centrale simple sur  $K$ . Pour  
que  $A$  possède une involution (fixant  $K$ ), il faut  
et il suffit que  $2[A] = 0$  ds  $\text{Br}(K)$ .

Théorème (Albert)

Soit  $L/K$  une ext. quadratique et soit  $A$  une  
 $L$ -algèbre centrale simple. 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<sup>er</sup> théorème

\* définit un isomorphisme  $A \rightarrow A^\circ$   
 donc  $[A] = [A^\circ]$  ds  $\text{Br}(K)$  alg opposée  
 $= -[A]$ .

Réciproquement, <sup>supposons que</sup>  $[A] = [A^\circ]$ .

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 <sup>séparable</sup> corps  $\sqrt{\text{commutatif}}$  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  $x \mapsto i(x)$  de  $A$  sur  $L$ .  
 $i_L = \text{rest. de } i \text{ à } L$  est un isomorphisme de  $L$  sur  $i(L)$ .

Donc il existe (Skolem-Noether)  $a \in A^\times$  tel que  $i(x) = a x a^{-1}$  pour tout  $x$  de  $L$ .

L'anti-isomorphisme  $x \mapsto a^{-1} i(x) a$  possède la propriété voulue en a).

(b) est un énoncé géométrique: il se vérifie q'après ext. des scalaires. Alors  $A$  devient  $M_n(K)$  et  $L$  devient l'algèbre diagonale  $K \times \dots \times K \hookrightarrow M_n(K)$ .

Soit  $i$  un anti-isomorphisme  $A \rightarrow A$ .

Il existe  $a \in A^\times$  tq  $i(x) = a^t x a^{-1}$ .

$$a^t x a^{-1} = x \quad x \in L$$

$$\Rightarrow a \text{ commute à } L$$

$$\Rightarrow a \in L^\times \quad a = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

$$\text{d'où } i^2(x) = a (a^{-1} x a) a^{-1} = x.$$

Si  $[A] = [A^0] \Rightarrow$  involution existe | de type  $\perp$  (n pair)  
 | de type alterné (n pair)

la méthode donne  $\perp$  par construction.

Pour le type alterné, il s'en déduit :

$\Rightarrow$  \* type  $\perp$ ,

on choisit  $a \in A^\times$  avec  $a^* = -a$ . (existence n pair)

$x^I = a x^* a^{-1}$  définit une involution de type symplectique.



Reste à choisir  $a \in A^*$   $a^* = -a$

$a \in A^*$ : donne un ouvert de Zariski de  $A$ .

Supposons  $K$  infini

Soit  $A_-$  l'ensemble des éléments anti-invariants par  $*$ . On doit voir que  $A_-$  rencontre cet ouvert. Il suffit de le voir après extension des scalaires OK si  $n$  pair.

Si  $K$  fini  $A$  est une alg. de matrices d'où existe formes alt non dégénérées si  $n$  pair.

Remarque:  $A$  invol., simple de centre  $K$   $\text{rg} = n^2$   
 $A_+ = \{a, a^* = a\}$   $\dim A_+ = \frac{n(n+1)}{2}$   
 dans le cas orthogonal

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

dans le cas symplectique

2<sup>e</sup> thm: preuve

$A$  centrale simple sur  $L$ ,  $L/K$  quadratique  
 $K$ -involutions de 2<sup>e</sup> espèce, non triviales sur  $L$

$A$  sur  $L$

$\lambda \mapsto \bar{\lambda}$  invol de  $L$

$\otimes \bar{A}$  algèbre réduite de  $A$  par changement de base  $L \xrightarrow{\lambda \mapsto \bar{\lambda}} \bar{L}$ .



② A vue comme L-algèbre par  $L \xrightarrow{\bar{\cdot}} L \xrightarrow{\cdot} A$ . (154)

③  $\bar{a} \in \bar{A}$

$$(\overline{ab}) = \bar{a} \bar{b}$$

$$\overline{\lambda a} = \bar{\lambda} \bar{a} \quad \lambda \in L$$

Une involution de 2<sup>e</sup> espèce définit un  
anti-isomorphisme  $A \rightarrow A$ , ie  $A^o = \bar{A}$ .  
d'où condition nécessaire ds  $\mathcal{P}_R$

$$[A^o] = [\bar{A}] \text{ ds } \mathcal{P}_R(L)$$

$$\text{ie } [A] + [\bar{A}] = 0. \quad (+)$$

Soit A satisfaisant à  $[A] + [\bar{A}] = 0$ .

Il existe  $i: A \rightarrow A$  tq  $i(xy) = i(y)i(x)$   
 $i(\lambda) = \bar{\lambda} \quad \lambda \in L$ .

$\left\{ \begin{array}{l} i: \text{anti-linéaire} \\ \text{anti-isomorphisme.} \end{array} \right.$

Si i est comme ci-dessus,

$x \mapsto i^2(x)$  L-automorphisme de A.

Il existe  $a \in A^\times$  tq  $i^2(x) = a x a^{-1} \quad \forall x \in A$

$$i^3(x) = i(i^2(x)) = i(a^{-1}) i(x) i(a)$$

$$= i^2(i(x)) = a i(x) a^{-1}$$

$$\Rightarrow \text{Il existe } \lambda \in L^\times \quad \begin{aligned} \lambda &= a i(a) \\ &= i(a) a \end{aligned}$$

$$i(\lambda) = i^2(a) i(a) = a i(a) = \lambda$$

donc  $\lambda \in K^\times$ .



Que donnent d'autres choix?

$a \mapsto \mu a$   $\mu \in L^\times$   $\lambda$  défini à  $NL^\times$  près.

On peut aussi changer de  $i$ , mais en fait:

$\lambda$  vu comme elt de  $K^\times / NL^\times$  ne dépend ni du chx de  $a$ , ni de celui de  $i$ .

$i'(x) = bi(x)b^{-1}$  et calcul. (cf Scharlau)

$$K^\times / NL^\times = \text{Br}(L/K) = \text{Ker: } \text{Br } K \rightarrow \text{Br } L.$$

Lemme. L'élément  $(\lambda) \in \text{Br}(L/K)$  est le Cor  $[A]_{L/K}$

Si une invol existe,  $a=1$   $\lambda=1 \Rightarrow \text{Cor}=0$

Invers<sup>t</sup> si  $\text{Cor}=0$ ,  $\lambda = \mu \bar{\mu}$

on chge pr que  $\lambda=1$ ,  $a i(a) = 1$ .

on chge de  $i$  !

$$i \mapsto bi b^{-1} \quad \mathcal{I}(x) = bi(x)b^{-1}$$

$$\mathcal{I}^2(x) =$$

(voir p. 158, Correction)

$$= b i(b^{-1}) a x a^{-1} i(b) b^{-1}$$

d'où  $bi(b^{-1}) = a^{-1}$  ie  $a \in \text{Im}(i-1)$ . ok

Preuve du lemme  $B$  alg sur  $L$  (quad /  $K$ )

$$\text{Vect}_L \longrightarrow \text{Vect}_{L/K}$$

$V \otimes_L \bar{V}$   $\text{Gal}(L/K)$  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 descente  $\bar{\phantom{x}}$  Weil.

On devrait appeler ceci  $N_{L/K} V$  "norme" de  $V$ .

[Par contre  $\text{Tr}_{L/K} V = V$  vu comme  $K$ -esp. vectoriel obtenu par descente  $\bar{\phantom{x}}$  par rapport à la somme directe des conjugués -]

$$\text{On a } N(V \otimes V') = N(V) \otimes N(V').$$

$B$  alg sur  $L \rightarrow \text{Cor } B = \text{une } K\text{-alg. de } B \otimes_L \bar{B}$   
formée des invariants  
de  $\sum g_i \otimes \bar{g}_i \mapsto \sum g_i \otimes \bar{g}_i$   
(cf. Riehm, Inv.).

$$A \otimes_L \bar{A} = \Delta \otimes_K L \quad \Delta = \text{Cores } A$$

$H$  alg. de quaternions définie par  $(L/K, \lambda)$

$$H = L \oplus L \cdot \varphi \quad \varphi^2 = \lambda$$

$$\varphi \varphi^{-1} = \mathbb{I} \text{ pour tout } \ell \in L$$

On va voir que  $\Delta \otimes_K H$  est isomorphe à une alg. de matrices, d'où  $[\Delta] + [H] = 0 \Rightarrow [\Delta] = [H]$

$$\text{On a: } \dim_K \Delta = n^2 \quad \dim_K H = 4$$

$$\dim_K A = 2n$$



On définit deux plongements

$$\Delta \longrightarrow \text{End}_K A (\simeq M_{2n}(K))$$

$$H \longrightarrow \text{End}_K A$$

de sorte que les images soient le commutant l'une de l'autre d'où isomorphisme voulu

$$\Delta \otimes_K H \simeq \text{End}_K A.$$

(car les dimensions sont bonnes).

$$\Delta \subset A \otimes \bar{A}$$

$$A \otimes_L \bar{A} \longrightarrow \text{End}_K A$$

$$x \otimes \bar{y} \longmapsto u_{x, \bar{y}}(z) = x z i(y) \quad z \in A$$

$$H = L \oplus L\varphi \quad \varphi^2 = \lambda$$

$$L \longrightarrow \text{End } A$$

$$\varphi \longmapsto \underline{\varphi} \in \text{End } A \quad \underline{\varphi}(z) = i(z) a \quad z \in A$$

Vérifions:  $\underline{\varphi}^2(z) = i(i(z) a) a = i(a) i^2(z) a = i(a) a z a^{-1} a = \lambda z.$

On a de plus  $u_{x, \bar{y}} \circ \varphi = \varphi \circ u_{y, \bar{x}}$ , d'où le fait que les

images de  $\Delta$  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~~  $q > 62$ )  
et peut ~~être~~ <sup>marche dès que</sup> mieux.

$$\begin{array}{c} A_S \\ \downarrow \\ \mathbb{P}_1 \end{array}$$

2) A de 2<sup>e</sup> espèce  $aa^* = 1 \Rightarrow a \stackrel{?}{=} b^{-1}b^*$

① On pourrait supposer que A est un corps (gauche)  
 $\text{Cor} = 0$ .

② Si  $a = -1 \Rightarrow i^2(x) = axa^{-1} = x$ , i involution

③ Si  $1+a$  est inversible et  $b = \frac{1}{1+a}$  convient

$$b^* = \frac{1}{1+a^{-1}} = \frac{a}{1+a} \quad b^{-1}b^* = a$$

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

$$\underline{H}_A(K) = H_A$$

$$\underline{H}_{-A}(K') = H_{A \otimes_K K'}$$



$$U_A \subset GL_A \text{ (groupe multiplicatif de } A) \quad (159)$$

$$GL_A(K') = (A \otimes_K K')^{\times}$$

hermitiens inversibles  $H_A^{\times}$ .

Th:  $\boxed{GL_A / U_A \simeq H_A^{\times}}$  (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  $H_A$  (en particulier  $H_A^{\times}$ ).

L'action sur  $H_A^{\times}$  est transitive et le stabilisateur de  $h = 1$  est  $U_A$ .

montrer:

$$GL_A \longrightarrow H_A^{\times} \text{ lisse}$$

$$x \longmapsto x \cdot 1 \cdot x^* = x x^*$$

L'application tangente à l'origine :

$$x = 1 + \varepsilon$$

$$\begin{cases} \varepsilon^2 = 0 \\ \varepsilon \varepsilon^* = 0 \end{cases}$$

$$A \longrightarrow H_A$$

$$\varepsilon \longmapsto \varepsilon + \varepsilon^*$$

surjective

$$(1 + \varepsilon)(1 + \varepsilon^*) = \dots$$

car :  $\varepsilon + \varepsilon^* = \eta$   $\varepsilon = \frac{1}{2} \eta$  marche

Plus généralement:

$$GL_A \longrightarrow H_A^{\times}$$

$$x \longmapsto x h x^* \quad h \in H_A^{\times}$$

L'appl. tgl<sup>e</sup> 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:

$$\varepsilon h + h \varepsilon^* = \frac{1}{2} \eta + \frac{1}{2} h (h^{*-1} \eta^*)$$

$$= \frac{1}{2} \eta + \frac{1}{2} \eta = \eta.]$$



d'appl. tgle est surjective, les orbites sont ouvertes

$H_A^x$  ouvert d'un ev., irréductible, connexe donc il y a une seule orbite. Soit le résidu

Tout elt hermitien <sup>inversible</sup> est donc du type  $x x^*$  après extension des scalaires.

Ce point se démontre en fait directement: si  $K$  alg. cl. s, tout hermitien <sup>inv.</sup> est le carré d'un hermitien. En effet

Lemme si  $K$  alg. cl. s de car  $\neq 2$  et si  $E$  est une alg. de dim finie sur  $K$ , si elt inversible de  $E$  est un carré.

(On applique  $\bar{\phantom{x}}$  à  $E =$  alg eng. par un elt hermitien)

$$1 \rightarrow \underline{U}_A \rightarrow GL_A \rightarrow H_A^x \rightarrow 1$$

espace homogène

$$A^x \rightarrow H^0(K, H_A^x) \rightarrow H^1(K, \underline{U}_A) \rightarrow H^1(K, GL_A)$$

$\parallel$   $\parallel$  "thm 9.0"

$H_A^x$   $0$

cf LN 5 Interprétation de la suite exacte:

$H^1(K, \underline{U}_A) \simeq H_A^x / \text{action de } A^x$

action de  $A^x$ :  $a \in A^x \quad h \mapsto a h a^*$



classes de  
modules hermitiens  $\simeq \mathcal{H}'(K, U_A)$   
de rang 1 non  
dégénérés

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 ds le cas de dim finie!).

Cas particulier  $M$  libre de rang 1.  $M = Ae$

$h(e, e)$  suffit pour tout connaître

$$h = h(e, e) \in H_A^*$$

Chgt de base le transforme en  $a h a^*$



$\text{Aut } A$  "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  $\bar{a} = -a$  (" $\bar{\phantom{x}}$ " = invol. stand)]

On pose:  $x^* = a \bar{x} a^{-1}$ .

Par un choix convenable de l'involution (bcp de places ramifiées, au - 4 marche).



principe de Hasse faux ("c'est le seul cas"). (163)

## ② Invariants de tenseurs quadrotiques

$V$  esp. vect. de dim finie sur  $K$

Soient  $v_i$  des "tenseurs quadrotiques" ie des éléments de  $\otimes^2 V$ ,  $V \otimes V'$ ,  $\otimes^2 V'$ .

Soit  $G_v$  le fixateur de ces éléments  $\subset GL_V$ .  
Alors  $G_v$  est isomorphe au groupe unitaire  $U_A$  d'une algèbre  $\bar{\alpha}$  invol. conserv.

Cor intersection de gpes orthog (et symplectiques) est un gpe unitaire.

Rq: cubique ne marche pas

- $G_2$  rep. lié à  $d^0 7$   
forme trilineaire alternée  $\dots \rightarrow G_2 \times \mu_3$
- $E_6$  est aussi possible (rep. de  $d^0 27$ ).

Application par Eva à ex de ppe Hasse faux.

Preuve de ②:

On va construire une alg.  $\bar{\alpha}$  involut  $A$

$$A \subset \text{End}(V) \times \text{End}(V') = R \quad V' = \text{dual}$$
$$(f, g) \mapsto ({}^+g, {}^t f)$$

Pour tout tenseur  $v$  quadrotique, on va définir  $A_v \subset R$

$$\textcircled{a} \quad v \in V \otimes V' = \text{End}(V)$$
$$V \xrightarrow{v} V$$



$$A_v = \{ (f, g), \text{ avec } f v = v f, \text{ et } {}^t g v = v {}^t g \}.$$

$$(f, g)$$

fixateur de  $v$  est égal à  $U_{A_v}$

$$\text{ici } f v f^{-1} = v$$

$$f v = v f$$

$$U_R = \{ (f, {}^t f^{-1}) \} \quad f \in GL(V)$$

$$\textcircled{b} \quad v \in V \otimes V$$

$$\text{Hom}(V, V')$$

$$\begin{array}{ccc} V & \xrightarrow{v} & V' \\ f \downarrow & & \downarrow g \\ V & \xrightarrow{v} & V' \end{array}$$

$$A_v = \{ (f, g) \mid \begin{array}{l} g v = v f \\ {}^t f v = v {}^t g \end{array} \}$$

On vérifie que ceci définit alg à invol et que le fixateur est le gpe unitaire

Grâce aux "2 cond" ne dépend pas de la manière de voir  $v$  comme hom.

$$\textcircled{c} \quad v \in V' \otimes V' \text{ m\u00eame chose.}$$

ou encore  $v$  interpr\u00e9t\u00e9 comme forme bil\u00e9aire

$$B_v: V \times V \rightarrow K$$

$$(f, g) \in R_v \iff \begin{cases} B_v(fx, y) = B_v(x, {}^t g y) \\ B_v(gx, y) = B_v(x, {}^t f y) \end{cases} \quad \forall x, y.$$



Problème

Existe-t-il un plongement de  $G_2$  dans  
un groupe semi-simple  $G$  et des sous-  
 $H_2$  de  $G$  isom. à sous- $so$  (ou sympl.)  
tels que  $G_2 = \cap H_2$  ?

(En particu. on ne demande plus alg. général  
ds un GL avec l'ident. usuelle).

en g.al : on plonge ds  $\cap$  quadriques.

Théorème (Bayer-Lensstra) Soit  $A$  une  $K$ -algèbre  
à inv. Soit  $K' / K$  une ext. de  $d^0$  impair  
Alors  $H^1(K, \underline{U}_A) \rightarrow H^1(K', \underline{U}_A)$  est injective.

Plusieurs réductions :

$\rightarrow$  radical.

$$\begin{cases} \Gamma_A \subset A \\ \Gamma_A \text{ idéal nilpotent} \end{cases} \quad \begin{cases} A / \Gamma_A \text{ semi-simple} \end{cases}$$

Th :  $H^1(K, \underline{U}_A) \rightarrow H^1(K, \underline{U}_{A/\Gamma})$  est  
bijective

Par ex : en interprétant avec les hermitiens  
(inversible  $\Leftrightarrow$  image mod rad. inv.).

Ou encore

$$1 \rightarrow N \rightarrow \underline{U}_A \rightarrow \underline{U}_{A/\Gamma} \rightarrow 1$$

$N =$  nilpotent déployé = ext. succ. de  $\mathbb{G}_a$   
donc à cohom. triviale.



On peut supposer  $K' = K(x)$  monogène

On choisit un tel  $x$ , d'où une forme linéaire  $\lambda : K' \rightarrow K$ ,  $\lambda(1) = 1$  et  $\lambda(x^i) = 0$ ,  $1 \leq i \leq m$

$M_1$  et  $M_2$  modules hermitiens sur  $A$  non dégénérée libre de rang 1.

$$K' \otimes M_1 \simeq K' \otimes M_2 \Rightarrow M_1 \simeq M_2$$

Si  $M'$  est un  $A'$ -module hermitien de

rang 1, on définit  $\lambda(M')$ ,  $A$ -module hermitien de rang  $n = [K':K]$  par :

$$\lambda(M') = M' \text{ comme } A\text{-module}$$

$$\begin{array}{ccc} M' \times M' & \longrightarrow & A \\ & \searrow & \uparrow 1 \otimes 1 \\ & & A' \\ & & \parallel \\ & & K' \otimes A \end{array}$$

$$M'_1 = K' \otimes M_1$$

$$\downarrow$$

$$N_1 = \lambda(M'_1) \text{ de rang } n \text{ sur } A.$$

On peut donner la structure de ce module

$K'$  esp. quad. sur  $K$

$$(x, y) \mapsto \lambda(xy)$$



$$K' \simeq \langle 1, 1, -1, 1, -1, \dots, 1, -1 \rangle$$

$$\simeq \langle 1 \rangle + \mathbb{R}$$

hyperbolique

$$K' = K1 \oplus H' \oplus H''$$

↑  
total isot

$$N_1 \simeq M_1 \oplus \underbrace{H'_1 \oplus H''_1}_{\text{total isotropes}}$$

libres de rg  $\frac{m-1}{2}$

idem pour  $N_2$

$$H'_1 \oplus H''_1 \simeq H'_2 \oplus H''_2$$

Thme de simplification de Witt est vrai ds le cas hermitien (cf exposé d'Eva ci-après).

d'où  $M_1 \simeq M_2$

Fin de la réduction

$$H^1(K, U_A) \rightarrow H^1(K', U_A) \quad \text{injective}$$

$K' / K$  d'° impa

On peut supposer que  $A$  est semi-simple, en fait m algèbre à involution simple:

$$A = A_1 \times \dots \times A_r \times A_{r+1} \times A_{r+1}^* \times \dots \times A_s \times A_s^*$$

[Certaines sont invariantes par involution.  $A_i = A_i^*$   
D'autres échangées.

$$H^1(K, U_A) = H^1(K, A_1) \times \dots \times H^1(K, U_{A_r})$$

$$\times \underbrace{H^1(K, U_{A_{r+1} \times A_{r+1}^*})}_{\text{"0."}} \times \dots \times \underbrace{H^1(K, A_s \times U_{A_{s+1} \times A_{s+1}^*})}_{\text{"0."}}$$

$$U_{B \times B^*} = \text{Gl}_B \quad \text{et "Hilbert 90".}$$

Reste à démontrer ce qu'on veut pour  $A$  une  $K$ -algèbre à involution simple.

Thème (Bak, 1969): Si  $N_1$  et  $N_2$  sont des modules hermitiens, tels que

$$N_1 \oplus H(A) \cong N_2 \oplus H(A)$$

$H(A)$  plan hyperbolique sur  $A$ .

$$= Ax \oplus Ay \quad \text{muni de} \quad \begin{aligned} \langle x, x \rangle &= \langle y, y \rangle = 0. \\ \langle x, y \rangle &= 1 \end{aligned}$$

Alors  $N_1 \cong N_2$

Reques:  $\langle , \rangle = h$  ds la notation antérieure  
On suppose ts les mod hermitiens non dégénérés (vrais ab aut



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  $N \oplus M \cong A^n$

$$\text{d'où } N_1 \oplus H(A)^n \cong N_2 \oplus H(A)^n$$

et par récurrence se déduit du thme énoncé.

Ref: B. Keller Math. Zeit. 198 1988.

M. Knus livre à paraître chez Springer.  
(Quebbemana, Scharlau, W. Scharlau, Schulte,  
Mémoires SMF ~ 1976 très général).

### Démonstration

$M = N \oplus H(A)$  forme hermitienne  $\langle, \rangle$

$(x, y)$  paire hyperbolique

Lemme  $U(M)$  agit transitivement sur  
l'ensemble des plans hyperboliques  
de  $M$ .

lemme  $\Rightarrow$  théorème

$$M = N_1 \oplus H_1 = N_2 \oplus H_2$$

$$\varphi: M \rightarrow M \quad \varphi(H_1) = H_2, \text{ alors } \varphi(H_1^\perp) = H_2^\perp$$

$\begin{matrix} \text{"} \\ N_1 \end{matrix} \qquad \begin{matrix} \text{"} \\ N_2 \end{matrix}$



## Transvections $(M, \langle \rangle)$

(170)

Soient

$$u \in M \quad \langle u, u \rangle = 0.$$

$$v \in M \quad \langle u, v \rangle = 0.$$

$$a \in A \quad \text{tel que } a + \bar{a} = \langle v, v \rangle.$$

Posons :  $\sigma_{u, a, v}(x) = x + \langle x, v \rangle u - \langle x, u \rangle v - \langle x, u \rangle a$

Lemme : 1) C'est une isométrie :  $\sigma_{u, a, v} \in U(M)$ .

$$2) \quad \varphi \sigma_{u, a, v} \varphi^{-1} = \sigma_{\varphi(u), a, \varphi(v)}$$

pour tout  $\varphi \in U(M)$ .

$$3) \quad \sigma_{u, a', v} \circ \sigma_{u, a, v} = \sigma_{u, a + a', v}$$

Vérification par calcul direct.

## Isométries hyperboliques

$$M = N \oplus H$$

isométrie de  $H$  étendue à  $M$  par identité

$H = H(A)$  avec paire hyperbolique  $x, y$

$$\alpha \in A^* \quad H_{x, y}(\alpha) \in U(H) \subset U(M)$$

$$H_{x, y}(\alpha)(x) = \alpha x$$

$$H_{x, y}(\alpha)(y) = \bar{\alpha}^{-1} y$$

On note  $G(M, x, y)$  le sous-groupe de  $U(M)$  engendré par les transvections  $\sigma_{u, a, v}$  avec  $u \in Ax \cup Ay$   $v \in N$  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  $\varphi \in G(M, x, y)$  tq  
 $\varphi(x) = x'$  et  $\varphi(y) = y'$ .

Démonstration

$$0 = \langle x', x' \rangle = \alpha \bar{\beta} + \beta \bar{\alpha} + \langle u, u \rangle$$

$$\text{d'où } \langle u, u \rangle = -\alpha \bar{\beta} - \beta \bar{\alpha}.$$

$$\langle \alpha^{-1} u, \alpha^{-1} u \rangle = -\bar{\beta} \bar{\alpha}^{-1} - \alpha^{-1} \beta$$

$$\sigma_{y, -\alpha^{-1} \beta, -\alpha^{-1} u} \in G(M, x, y)$$

$$\sigma_{y, -\alpha^{-1} \beta, -\alpha^{-1} u}(x) = \alpha^{-1} x'$$

$$\psi = H_{x, y}(\alpha) \circ \sigma_{y, -\alpha^{-1} \beta, -\alpha^{-1} u}$$

$$\psi^{-1}(y') = \gamma x + \delta y + v$$

$$\langle \psi^{-1}(x), \psi^{-1}(y') \rangle = 1 = \langle x, \gamma x + \delta y + v \rangle = \delta$$

$$\langle v, v \rangle = -\gamma - \bar{\gamma}$$

$$\sigma_{x, -\gamma, -v}(x) = x$$

$$\sigma_{x, -\gamma, -v}(y) = \psi^{-1}(y').$$



Posons  $\varphi = \psi \circ \sigma_{x, -x, -v}$

On a :  $\varphi(x) = x'$

$\varphi(y) = y'$

Remarque. Soit  $z \in N$ ,  $\langle z, z \rangle = \rho + \bar{\rho}$   
 $\sigma_{x, \rho, z}(x') = (\alpha - \beta\rho + \langle u, z \rangle)x + \dots$

Donc il suffit de trouver un  $z$  dans  $N$   
 tq  $\begin{cases} (\alpha - \beta\rho + \langle u, z \rangle) \text{ soit inversible.} \\ \langle z, z \rangle = \rho + \bar{\rho} \end{cases}$

• Corps gauches  $A = \mathbb{D}$ .

Soit  $(x', y')$  une "autre paire".

$x' = \alpha x + \beta y + u$

Si  $\alpha \neq 0$  OK.

Sinon il faut trouver  $z \in N$   $\langle u, z \rangle - \beta\rho \neq 0$ .  
 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,  $M \neq H(A)^n$ .

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  $G(\pi, x_i, y_i)$

Lemme  $G$  agit transitivement sur l'ensemble  
des  $n$ -uples de paires hyperboliques



# Orthogonaux deux à deux.

173

Démonst. par récurrence

Algèbres simples

Soit  $D$  un corps gauche muni d'une involution  $D \rightarrow D$

$A = M_n(D)$  et soit  $*$   $A \rightarrow A$  involution donnée par  $(d_{ij})^* = (\overline{d_{ji}})$ .

Soient  $e_{ij} = \begin{pmatrix} 0 & \vdots & 0 \\ & 1 & \\ 0 & \vdots & 0 \end{pmatrix}$

$e_{11} =: e$  Soit  $M = N \oplus H$  un module hermitien et  $(x, y)$  une paire hyperbolique de  $H (\cong H(A))$

Proposition 1)  $(eM, \langle, \rangle|_{eM})$  est un module hermitien sur  $D = eAe$

2)  $eH$  est la somme  $\perp$  de  $n$  plans hyperboliques  $H_i \cong H(D)$  avec paire hyperbolique  $(e_{1i}x, e_{1i}y)$ .

3) Tout élément de  $U(eM)$  s'étend de façon unique en un élément de  $U(M)$ .

Rqve:  $e = e_{11}$  est bien un projecteur hermitien.



## Théorème

(174)

- 1)  $G(e\pi, e, x, e, y) \subset G(\pi, x, y)$
- 2)  $G(\pi, x, y)$  agit transitivement sur l'ensemble des paires hyperboliques.

## Démonstration

Montrons que les extensions des générateurs sont dans  $G(\pi, x, y)$ .

- Clair pour ceux de la forme  $H(\alpha)$
- $\sigma_{z, a, u}$  une transvection associée à  $H_i$  plan hyperbolique engendré par  $e_{1i}x, e_{1i}y$   
 $z = e_{1i}x$  ou  $e_{1i}y$  ou multiple  
et  $u \in H_i^+$ .

Si  $u \in H^+ = N$   $\sigma_{z, a, u} \in G(\pi, x, y)$

sinon soit  $u = v + w$  avec  $v \in H$   
 $w \in H^+ = N$

$$\sigma_{z, a, u} = \sigma_{z, b, v} \circ \sigma_{z, c, w} \quad \begin{cases} b + b^* \leq v \\ c + c^* \leq w, u \end{cases}$$

$$\sigma_{z, c, w} \in G(\pi, x, y)$$

$$\sigma_{z, b, v}(x) = \alpha'x + \beta'y \quad \text{On voit que } \alpha' \in A^\times$$

Il existe par la proposition du début un

$$\begin{aligned} \varphi \in U(H) & \text{ avec } \varphi(x) = x' & \varphi(y) = y' \\ \varphi \in G(H, x, y) & & \\ \text{donc } \varphi &= \sigma_{z, b, v} \end{aligned}$$



Reste le cas où l'involution  $\sim$  est quelconque  
 Il existe une unité  $c \in A^\times$  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  $(x, c^{-1}y)$  est une paire  
 hyperbolique pour  $(M, <, >_c)$ .

3) Les sous-groupes du groupe unitaire  
 se correspondent.

$$G(M, <, >, x, y) = G(M, <, >_c, x, c^{-1}y).$$



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  
galoisienne sur  $K$

Exemple 2  $V$  base  $(e_g)_{g \in G}$ ,

$$g e_h = e_{gh} \quad (\text{à gauche})$$

$q$  forme quadratique telle que  $e_g$  base  
orthonormale.

$$q(e_g, e_{g'}) = \begin{cases} 0 & g \neq g' \\ 1 & g = g' \end{cases}$$

"G - forme quadratique unitaire"

il existe un vecteur  $e \in V$  tel que

$e_g \quad (g \in G)$  base de  $V$

$$q(e, e_g) = \begin{cases} 0 & \text{si } g \neq 1 \\ 1 & \text{si } g = 1 \end{cases}$$

$L/K$  a une base normale antiduale (BNA)

"belle base"



Si:  $(L, q_L, \text{action de } G) \simeq G\text{-forme quadratique unitaire}$

$\Leftrightarrow$  il existe  $e \in L$ , tel que:

$(ge)$  base de  $L$

$$\text{Tr}(e \cdot ge) = \begin{cases} 0 & \text{si } g \neq 1 \\ 1 & \text{si } g = 1 \end{cases}$$

Il n'est pas comode de rester dans le cadre des extensions de corps.

### "G-algèbre galoisienne"

$n \geq 1$ ;  $K$  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  $G$ -espace sur  $K$  (espace principal homogène à droite sur  $G$ )

[ $L$  sert à l'ordre des objets où opère  $G$ .]



- (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 <sup>s. trans.</sup> 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, extensions galoisiennes de degré fini de  $K$ , permutes par  $G$ .

Réclame :

- (1) ext. des scalaires  $L/K$   $G$ -gal  
 $K'/K$  ext,  $L \otimes_K K'$   $G$ -alg. gal.
- (2) Induction :  
 Si  $\varphi: G \rightarrow G'$  est un homomorphisme de groupes finis, toute  $G$ -algèbre galoisienne définit une  $G'$ -algèbre galoisienne 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



$H \subset G$ , alg. ind:  $\text{Ind}_H^G(K_H)$

Pour toute  $G$ -algèbre galoisienne, il existe un s/g  $H$  de  $G$  (défini à conj. près) et une ext. gal.  $K_H$  de  $K$  à groupe de Galois  $H$ , telle que  $L = \text{Ind}_H^G(K_H)$ .

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 "belle base" pour  $G$ -alg. gal.  $L$ ?

Plus généralement:

$G$ -forme quadratique  $\stackrel{?}{=} \text{forme unitaire}$ ?

Condition nécessaire:

$(V, q)$  repr. de  $G$  ds  $V \simeq$  repr. régulière (\*)

Lemme:

Si  $K$  est algébriquement clos,  $(*) \Leftrightarrow$   
forme unitaire.

$$e \in V, \quad q(e, ge) = 0 \quad g \in G, g \neq 1$$

$$q(e, e) = 1.$$

forme quadratique  $q_g(x) = q(x, gx)$   $n-1$  formes  
 $n-1 < n$ , donc  $\exists e \neq 0, e \in V$   
 comme ci-dessus. (se démontre avec les formes hermitiennes)  
 $q(e, e) \neq 0$

$G$ -formes quadratiques qui sont des "K-formes"  
 de la  $G$ -forme unitaire.

Automorphismes de la  $G$ -forme unitaire

Groupe unitaire  $V_A$  de l'algèbre à involution

$A = K[G]$ , munie de l'involution  $g^* = g^{-1}$

$$\sum a_g g \mapsto \sum a_g g^{-1}$$

$V$  base  $(ge)$   $e \in V$

Automorphisme  $u: e \mapsto \sum a_g ge$

$u$  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 unitaire par fonction 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

$L$  a classe de cohomologie  $u_L \in H^1(K, U_G)$  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'un tenseur de degré 2

$$V, q, g \in G$$

$$V^* \otimes V^* \quad V \otimes V^*$$

Corollaire 1:

Si  $L$  est une  $G$ -algèbre galoisienne, et  
si  $L \otimes_K K'$  a une belle base avec  $[K':K]$   
impair, alors  $L$  a une belle base.

On pourra donc supposer:

- ①  $K$  parfait
- ②  $G_K$  est un pro-2-groupe.

Corollaire 2:

Si  $G$  est d'ordre impair, alors  $L$   
a une belle base.

Propriété des algèbres galoisiennes ayant  
 une belle base:

$L$  une  $G$ -algèbre galoisienne.

$X$  "objet" = espace vectoriel muni de tenseurs  $v$ .

$L \hookrightarrow P$  "torseur" ( $= \text{Spec } L$ )

$X_P$  : tord. de  $X$  par  $P$

Donnée 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  
tenseurs sont de degré 2, alors  $X_P \simeq X$ .



$V, \alpha \rightarrow$  algèbre à involution  $R$

$$U_R = \text{Aut}(V, \alpha)$$

$$G \rightarrow U_R(K) \subset R$$

$$K[G] \rightarrow R \quad \text{compatible à l'involution}$$

$$U_G \rightarrow U_R$$

le cocycle " $L$ " étant trivial, son image dans  $U_R$  aussi.

Groupe d'ordre pair :

Remarque: Si  $K = \mathbb{R}$  (ou plus généralement corps ordonné maximal), une  $G$ -algèbre galoisienne est caractérisée par un élément  $s \in G$  (à conj. près) tel que  $s^2 = 1$

$$G_K \rightarrow G \quad \text{trivial ou inv.}$$

bonne base existe  $\Leftrightarrow s = 1$ .

$s \neq 1$ , forme trace de  $L$  a des lignes  $+$  et  $-$ ,  
en fait  $\cong \langle \underbrace{1, \dots, 1}_{n/2}, \underbrace{-1, \dots, -1}_{n/2} \rangle$

$$(L \cong \underbrace{\mathbb{C} \times \dots \times \mathbb{C}}_{n/2})$$

$s = 1 \Leftrightarrow L$  est (totale)ment réel



### Remarque:

S: l'ordre de  $G$  est pair, alors il existe (sur  $\mathbb{R}$ ) 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  $z \in H^1(G, \mathbb{Z}/2\mathbb{Z})$ , on a  $z_L = 0$  dans  $H^1(K, \mathbb{Z}/2\mathbb{Z})$ .

Lemme (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  $L$

$$e' = \sum_{h \in H} h e, \quad e' \in L^H$$

$$e'g = \sum_{h \in H} h g e \quad e'g \in L^H$$

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:

$$\text{Tr}_{L^H} \left( \sum_{h \in H} h x \cdot y \right) = \text{Tr}_L(xy) \quad x \in L, y \in L^H$$

### Autre démonstration:

forme trace de  $L^H$ : forme unité' de rang  $|G/H|$

tordue par l'action de  $G_A$  sur  $G/H$ , via  $G$ .

Or  $L$  "ne tord pas les tenseurs quadratiques".

- (2) Si  $L/K$  a une belle base, et si  $H \subset G$  est d'indice 2, alors l'image de  $G_K$  dans  $G$  est contenue dans  $H$ .

$L^H$  extension quadratique de  $K$

forme trace unité'

$$K(\sqrt{d}) \quad \langle 2, 2d \rangle \quad \text{discr} = d$$

forme trace unité'  $\Leftrightarrow d = 1$ , 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

$\Downarrow$

$K$  est un corps de  $\dim \leq 1$

(groupe de Brauer de tout ext. gal. de  $K$  est 0).

Thm (Steinberg) :

So  $K$  est parfait, de  $\dim \leq 1$ , alors  
 $H^1(K, B) = 0$  pour tout groupe algébrique  
lucarne convexe  $B$

$B = U_G^\circ$  : composante convexe de 1 dans  $U_G$ .

Lemme :

Le quotient  $U_G/U_G^\circ$  est de type  $(2, \dots, 2)$   
 (avec action de  $G_K$ ).

(Vrai pour tout groupe unitaire).

Liste des facteurs / clôture alg.

$GL_n, Sp_{2n}, O_n$

convexes, sauf  $O_n$ .  $O_n/SO_n$  de type  
 $(2, \dots, 2)$ .



$$G \longrightarrow U_G(K)$$

$$\searrow \quad \nearrow \\ U_G^0(K)$$

$$u_L \in H^1(K, U_G)$$

provient de  $u_L^0 \in H^1(K, U_G^0)$ , on a  $u_L^0 = 0$   
par Steinberg.

Variante :

Lemme (Bruxelles, 62)

Soit  $K'/K$  une extension quadratique de  
corps parfaits. Soit  $B$  réductif connexe.

Soit  $z \in H^1(K, B)$  donnant 0 dans  
 $H^1(K', B)$ .

Alors il existe un tore maximal  $T$  de  $B/K$   
et  $t \in H^1(K, T)$  donnant  $z$ .

$$\xi \in B(K'), \quad \xi \bar{\xi} = 1 \quad (- : \text{élément non triv. de } K'/K)$$

$$\xi \mapsto g^{-1} \xi \bar{g}, \quad g \in B(K')$$

On peut choisir  $\xi$  semi-simple régulier  
(condition ouverte). D'où un unique tore  
maximal  $T_{K'}$  contenant  $\xi$ . Mais  $\xi \in T$  aussi  
En fait,  $T_{K'}$ .  $\xi$  définit  $t \in H^1(K, T)$

# Parenthèse sur la structure de $U_G$

Hypothèse : car  $K = 0$   
 $K$  assez grand pour que les  
 repr. irréd. de  $G$  soient  
 définies sur  $K$   
 (par ex.  $K$  contenant les  
 racines  $n$ -ièmes de 1,  $n = |G|$ ).

$$K[G] = \prod M_\chi$$

$\chi$  car  
 irréd.

$$\cdot \chi = \overline{\chi}$$

$$\cdot \chi = \overline{\chi} \quad \left\{ \begin{array}{l} \text{repr. orthogonales} \\ \text{repr. symplectiques} \end{array} \right.$$

$$\cdot M_\chi \times M_\chi, \quad \text{involution échange les facteurs}$$

groupe unitaire :  $M_\chi^\times \cong GL_{n_\chi}$   
 et son  $H^1 = 0$

$$\cdot \text{Groupe unitaire} = O(q_\chi)$$

$$H^1 = \text{classes de f.q. de rang } n_\chi$$

$$G.n = Sp, \quad H^1 = 0$$



$$H'(K, U_G) \simeq \prod_{\substack{\chi \text{ de} \\ \text{type orth.}}} H'(K, O(q_\chi))$$

Le cas général est plus difficile, car on a des groupes unitaires sur des corps gardés munis d'involutions.

Exemple :

$$\boxed{G = A_4}, \quad A_4 / (2, 2) = C_3 \quad \omega_j: \mathbb{Q}(\sqrt{-3})$$

Supposons d'abord que  $\sqrt{-3} \in K$ .

$$A_G \simeq K \times K \times K \times M_3(K)$$

$$U_G \simeq \mu_2 \times G_m \times O_3$$

$$O_3 = O(q_3)$$

$$q_3 = \langle 1, 1, 1 \rangle$$

$L/K$  alg. gal. à groupe  $G = A_4$

$$u_L \in H^1(K, U_G)$$

Composante de  $(u_L)$  de  $\mu_2$  est 0

$$G_{1K} \rightarrow G \rightarrow U_G$$

$$G \rightarrow 1 \subset \mu_2$$

Composante de  $(u_L)$  de  $G_m$  est 0

composante de  $(u_L)$  de  $O_3 \hookrightarrow$

forme quadratique à 3 variables

$L \rightarrow K_4 = L^{A_3}$ , alg. étale 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  $\sqrt{-3} \notin K$  :

À la place 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:  $G = \text{Mouster}$ .

Corollaire ( $K$  corps de nombres)

Th. Soit  $L$  une  $G$ -algèbre galoisienne sur  $K$ ,  
 $G = A_n$ ,  $n \geq 4$ .  
 Alors,  $L$  a une belle base si et seulement si:

(a)  $L$  est totalement réelle

(b)  $G_K \rightarrow A_n$  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  $c$  ds  $\bar{A}_n$ ,  
 $c^2 = 1$ ,  $c \mapsto 1$  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 car.  $G_K \rightarrow \{\pm 1\}$ .

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:

Si  $L$  a une belle base, posons

$$K_n = L^{A_{n-1}}.$$

La forme trace est  $\langle 1, \dots, 1 \rangle$ .

Donc  $w_2 = 0$ . On sait que  $w_2$  est  
 l'obstruction à relever.

Démonstration:

Sous l'hypothèse plus forte que  $G = G'$ .

Th (M. Kneser):

Soit  $K$  un corps de nombres, et soit  $\mathbb{R}$   
 un groupe semi-simple convexe, simplement convexe,  
 n.



Soit  $z \in H^1(K, B)$ . Alors si  $z \mapsto 0$

pour tout plongement réel de  $K$ , alors  $z=0$ .

(Harder, Cernusov, Premet : cas exceptionnels).

$U_G^0$  : comp. neutre de  $U_G$   
c'est un groupe réductif connexe

$U_G^1$  : semi-simple connexe  
(groupe dérivé de  $U_G^0$ ).

$\tilde{U}_G^1$

$\downarrow$

$$U_G^1 \subset U_G^0 \subset U_G$$

$$u_L \in H^1(G_K, U_G), \quad G_K \rightarrow G \rightarrow U_G(K)$$

plongement évident.

On a déjà vu que l'image de  $G$   
est contenue dans  $U_G^0(K)$

Comme  $G = [G, G]$ , image est contenue  
dans  $U_G^1(K)$ .

$$\tilde{U}'_G(K)$$

$$\pi \downarrow$$

$$G \subset U'_G(K)$$

(3)  $G \subset \pi \tilde{U}'_G(K)$  . En effet,

$$1 \rightarrow C \rightarrow \tilde{U}'_G \rightarrow U'_G \rightarrow 1$$

$$\tilde{U}'_G(K) \rightarrow U'_G(K) \rightarrow H'(K, C)$$

$$\begin{array}{c} \uparrow \text{hom} \\ G \end{array}$$

$C$  est de type  $(2, \dots, 2)$  (avec action de Galois).

Donc  $H'(K, C)$  est abélien annulé par 2

Soit  $\tilde{G}$  l'image réciproque

$$\tilde{G} = \pi^{-1}(G), \text{ isom. } \tilde{a} \text{ } G \times C(K)$$

On a supposé  $H^2(G) = 0$ .

Donc  $G$  se relève

$$\tilde{G} \subset \tilde{U}_G(K)$$

$$\begin{array}{ccc} \downarrow \uparrow & & \downarrow \pi \\ G & \subset & U'_G(K) \end{array}$$



$\tilde{z}_L \in H^1(K, \tilde{U}_G')$  est 0?

$$\begin{array}{ccc} G_K & \rightarrow & G \\ c & \mapsto & 1 \end{array}$$

Un peu plus compliqué quand  $G \neq [G, G]$ .

Problème ouvert:

Généraliser ceci aux corps parfaits avec  $\text{cd}_2 K \leq 2$ .

Est-ce qu'il est vrai que si  $H^1 = H^2 = 0$ , une belle base existe?

Serait vrai si on savait :

$$\text{cd}(K) \leq 2 \Rightarrow H^1(K, \text{semi-simple connexe}) = 0$$

Dans cette direction, on a en tout cas :

Merkurjev - Suslin

$$\begin{aligned} \text{cd} \leq 2 &\Rightarrow D \text{ alg\`ebre centrale simple / } K, \\ K^* &= \text{Nrd } D^* \end{aligned}$$

Prochaine fois :

$$2\text{-Sylow ab. \textit{el'}. } \underbrace{(2, \dots, 2)}_{r \text{ facteurs}}$$

$G$ -algèbre galoisienne avec 2-groupe de Sylow abélien élémentaire.

Énoncé des résultats (Bayer-Serre, en préparation)

$K$  corps de car  $\neq 2$ ,  $G$  groupe fini,

$S$  2-Sylow de  $G$ ,  $N = N_G(S)$

$|G| = 2^r \cdot m$ ,  $m$  impair,  $2^r = |S|$

$L$   $G$ -algèbre galoisienne /  $K$

Existe-t-il une belle base ?

$q_L$  = forme trace de  $L$ , de rang  $2^r m$

① Th 1: Il existe une  $K$ -forme quadratique  $q_L^0$ , de rang  $2^r$ , et une seule à isom.

près, telle que

$$q_L \simeq m \otimes q_L^0 \quad (= q_L^0 \oplus \dots \oplus q_L^0, m \text{ fois})$$

Proposition:

Soit  $f$  une forme quadratique sur  $K$ , et

soit  $K'$  une extension finie de  $K$  de degré

impair. Soit  $m$  impair  $\geq 1$ .

Si  $f$  est divisible par  $m$  sur  $K'$ ,  $f$  est

divisible par  $m$  sur  $K$ .

Résulte des thm de Springer



$G_K \rightarrow G$  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  $q_L^0$  est la forme unité:  $q_L^0 = 2^r \otimes \langle 1 \rangle$ .

D'où condition nécessaire pour l'existence d'une belle base.

② Supposons  $S$  abélien élémentaire, de type  $(2, \dots, 2)$ , de rang  $r$ .

Th 2: La forme  $q_L^0$ , multipliée par  $2^r$ , est une  $r$ -forme de Pfister.

Autrement dit: si  $r$  est pair,  $q_L^0$  est une forme de Pfister, si  $r$  est impair,  $2q_L^0$  est une forme de Pfister.

Proposition (déjà vu)  
Si une forme quadratique devient une forme de Pfister par extension des scalaires, de degré impair, elle l'est déjà.



Th 3 : On fait 2 hypothèses :

(1)  $S$  est abélien élémentaire

(2) L'action de  $N/S$  sur  $S$  par conjugaison est transitive sur  $S - \{1\}$ .

Il y a alors équivalence entre :

(a)  $L$  a une belle base

(b)  $q_L^0$  est la forme unité  $\langle 1, \dots, 1 \rangle$

(b')  $2^r q_L^0$

$\langle 1, \dots, 1 \rangle$ .

Il est trivial que  $(a) \Rightarrow (b)$

$(b) \Rightarrow (b')$ , car  $2\langle 1, \dots, 1 \rangle \cong \langle 1, \dots, 1 \rangle$   
 $(\langle 2, 2 \rangle \cong \langle 1, 1 \rangle)$ .

### ③ Cohomologie de $G$

Prop : L'application de restriction

$$H^i(G) \rightarrow H^i(S)$$

est injective, et son image est formée  
 des éléments de  $H^i(S)$  qui sont invariants  
 par l'action de  $W = N/S$ .

(Résultat vrai chaque fois que le  
 2-sylow est abélien et  $G$ -module

2- $p$ -primaire (i.e.  $p=2$ ) à action triviale  
 de  $G$ )



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  $d^0 1$ .

Th 4: Il existe dans  $H^r(G)$  un élément

$z$  ayant la propriété suivante:

- La restriction de  $z$  à tout s/g de  $G$  d'ordre 2 est  $\neq 0$ .
- Cet élément est unique, à l'addition près de classes de cohomologie "négligeables".

$L$  est associé à un homomorphisme

$$\pi: G_K \rightarrow G. \quad \text{Si } x \in H^i(G),$$

$$\pi^* x \in H^i(G_K) = H^i(K).$$

$$\text{Je pose } x_L = \pi^* x \in H^i(K).$$

En particulier,  $z_L$  est un élément bien défini de  $H^r(K)$ , indépendant du choix de  $z$ .

Th 5: L'invariant cohomologique dans

$H^r(K)$  de la forme de Plister  $z^r q_L^0$

$$\text{est } z_L + (-1) \dots (-1) = z_L + e^r,$$

$$e = (-1) \in H^1(K).$$



$r$ -forme de Pfister :

$$\simeq \langle 1, -\alpha_1 \rangle \otimes \dots \otimes \langle 1, -\alpha_r \rangle = \langle \alpha_1, \dots, \alpha_r \rangle.$$

Son invariant d'Arason est  $(\alpha_1) \dots (\alpha_r) \in H^r(K)$

En particulier,  $\langle 1, \dots, 1 \rangle$  a pour invariant  
cohomologique  $(-1) \dots (-1) = 2^r \in H^r(K)$ .

Corollaire : La forme  $2^r q_L^0$  a même invariant  
cohomologique que la forme unit' 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 :

$r=0$   $G$  est d'ordre impair.  
Pas de condition — tjs belle base.

$r=1$  Si  $S = C_2$ , il existe  $G \xrightarrow{\mathbb{Z}} C_2 \rightarrow 1$

$$H^1(G) = \mathbb{Z}/2\mathbb{Z} \quad 1 \rightarrow H \rightarrow G \xrightarrow{G_K} C_2 \rightarrow 1$$

$z \in H^1(G)$  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

$$1 \rightarrow C_2 \rightarrow \tilde{G} \xrightarrow{\psi} G \rightarrow 1$$

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

$\psi^{-1}(S) \cong Q_8$ , 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  $\tilde{\pi}: G_K \rightarrow \tilde{G}$ .

Si  $G = A_4$  ou  $A_5$ , on retrouve  
que le relèvement à  $\tilde{A}_4, \tilde{A}_5$  est  
suffisant pour l'existence d'une belle base.

Si:  $G = \text{PSL}_2(\mathbb{F}_q)$ ,  $q \equiv \pm 3 \pmod{8}$ ,  
belle base  $\Leftrightarrow$  relèvement possible dans  
 $\tilde{G} = \text{SL}_2(\mathbb{F}_q)$ .

Un relèvement  $\tilde{\pi}$  définit une  $\tilde{G}$ -algèbre  
galoisienne  $\tilde{L}$ .

Th 7: Il existe un choix  $\tilde{\pi}$  (non unique  
en général) tel que  $\tilde{L}$  ait une belle  
base.

$v=3$  deux possibilités pour l'action de  
 $W = N/S$ . Si: transitive (sur éléments  $\neq 1$ )  
elle donne soit un groupe  $C_7$ , soit  
 $C_3 \cdot C_7$  (produit semi-direct, avec  $C_7$  normal).

Exemple:  $\text{SL}_2(\mathbb{F}_8)$ , 2-Sylow  $S = \mathbb{F}_8$

$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ ,  $N = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ ,  $N/S$  opère

par  $\mathbb{F}_8^* \cong C_7$ .



Groupe de Jacko  $J_1$ ,  $N$  agit par un groupe d'ordre 21.

(Noter que  $W = N/S$  est contenu dans  $SL_3(\mathbb{F}_2) = G_{168}$ , d'ordre impair, et que  $168 = 8 \cdot 21$ )

On peut décrire  $z$  explicitement.

On identifie  $S$  à  $\mathbb{F}_8$ , de sorte que l'action de  $N$  soit par homothétie (cas  $SL_2(\mathbb{F}_8)$ ), par homothétie et conjugaison (cas  $J_1$ ).

$z \in H^3(S)$ ? Polynôme de  $d^0 z$ .

On considère  $N_{\mathbb{F}_8/\mathbb{F}_2} = N$ .

C'est un polynôme cubique, après choix d'une base de  $\mathbb{F}_8$  sur  $\mathbb{F}_2$ .

$N(\lambda\tau) = N(\lambda)N(\tau)$ ,  $N(\lambda) = 1$  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  $\mathbb{Q}(T)$  à  
groupe de Galois  $G$ , ramifié en 3 points  
(conjugué par le corps cubique de disc.  $9^2$ ),  
la ramification étant d'ordre 3.

Si  $K$  est de car 0, et si  $t \in \mathbb{P}_1(K)$ ,  
distinct des 3 points de ramification,



$L_t$   $G$ -algèbre galoisienne sur  $K$  (spéc.)

D'où un invariant  $z_{L_t} \in H^3(K)$ .

Th : Cet invariant est  $(-1)(-1)(-1) = -1$ .

Donc  $L_t$  a une belle base



-1 est somme de 4 carrés dans  $K$ .

$L_T$  alg. gal. sur  $\mathbb{Q}(T)$

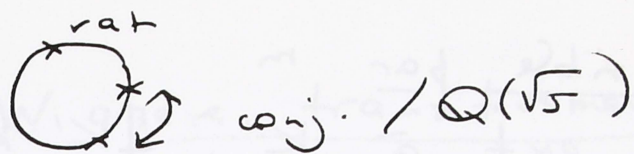
Invariant  $(-1)(-1)(-1) \in H^3(\mathbb{Q}(T))$ .

$z_{L_T} \in H^3(\mathbb{Q}(T))$



$J_1$ 

ramification d'ordre 2, 5, 5

Invariant :  $(-1)(-1)(-1)$ .Action non transitive $r \leq 3$  facile $r=3$ , action de  $W$  par  $C_3$ 

$$S = (2, 2) \oplus 2$$

$$\begin{array}{ccc} \hookrightarrow & & \uparrow \\ C_3 & & \text{fixe} \end{array}$$

Alors  $1 \rightarrow H \rightarrow G \rightarrow C_3 \rightarrow 1$ Il faut que  $\pi(G_K) \subset H$ (où  $\pi : G_K \rightarrow G$  corr. à  $L$ )et que la  $H$ -alg. gal. ait unebonne base : i.e.  $G_K \rightarrow H$  serelève en  $G_K \rightarrow \tilde{H} = 2H$ . $r > 3$  $q_L^0$  remplacé par "autant deformes 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  $2^r q_L^0$  est de Pfister.

Soit  $L_S$  une  $S$ -algèbre galoisienne

$S$  de type  $(2, \dots, 2)$

Si: corps,  $L_S = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_r})$

$L_S$  a pour base  $1, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_r}$   
 $\sqrt{\alpha_1}, \sqrt{\alpha_2}, \dots$

$$q_{L_S} \simeq 2^r \langle 1, \alpha_1, \alpha_2, \dots, \alpha_1 \alpha_2 \dots \rangle =$$

$$= 2^r \langle \langle -\alpha_1, \dots, -\alpha_r \rangle \rangle$$

Autre démonstration (plus simple)

$$L_S = K(\sqrt{\alpha_1}) \otimes \dots \otimes K(\sqrt{\alpha_r})$$

produit tensoriel de  $\langle 2, 2\alpha_i \rangle$ .

Th 2:  $2^r q_L^0$  est de Pfister

Il suffit de le voir sur  $K'$ ,

$\pi(G_K) \subset S$ ,  $L$  est induite d'une  
 $S$ -algèbre galoisienne  $L_S$



$$q_L = q_{L_S} \oplus \cdots \oplus q_{L_S} = n \otimes q_{L_S}$$

Th 3 : Si  $W$  opère transitivement sur  $S - \{1\}$ ,  
 alors  $q_L$  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 a 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.

$$S^1 = \text{Hom}(S, \{\pm 1\}) \simeq H^1(S)$$

d'ordre  $2^r$

$$L_S = \bigoplus L_S^{\chi}, \quad \dim L_S^{\chi} = 1.$$

$$L_S = L'_S \oplus \bigoplus_{\chi \neq 1} L_S^\chi$$

$L_S^\chi$  correspond à  $a(\chi) \in K^*/K^{*2}$

$$1_\chi : \langle e_\chi, e_\chi \rangle = 1$$

$$s e_\chi = \chi(s) e_\chi$$

$L_S$  a comme  $S$ -forme quadratique

$$2^r q_{L_S} = \langle 1 \rangle \oplus \sum_{\chi \neq 1} a(\chi) 1_\chi$$

$$\text{Ind}_S^N 2^r q_{L_S} = \text{Ind}_S^N \langle 1 \rangle \oplus \sum_{\chi \neq 1} a(\chi) \text{Ind}_S^N 1_\chi$$

$$w \in W = N/S$$

$$\text{Ind}_S^N 1_{w(\chi)} \cong \text{Ind}_S^N 1_\chi$$

$$\text{Ind}_S^N 2^r q_{L_S} = \text{Ind}_S^N \langle 1 \rangle \oplus \text{Ind}_S^N 1_\chi \otimes \sum_{\chi \neq 1} a(\chi)$$

On compare  $L_S$  à  $L_S^{\text{dép}}$

$$q_L^0 \cong \sum_{\chi \neq 1} a(\chi)$$



## Th 4 : Cohomologie

$$H^i(S, A)^{N/S}$$

$$H^i(G, A)_p \hookrightarrow H^i(S, A)_p^{N/S}$$

(i.e. 1. on  
coh. de  
Tate)

$A$  est un  $G$ -module

" $p$ " : composante  $p$ -primaire

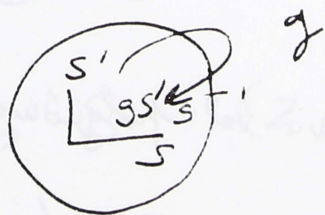
Thm : Si  $S$  est abélien et si l'action  
de  $G$  sur  $A$  est triviale, alors

$$H^i(G, A)_p = H^i(S, A)^{N/S}$$

Cartan - Eilenberg

"classe de cohomologie stable"

$z$  est stable si, pour tout  $s/g$   $s' \in S$   
et tout  $g \in G$ ,  $g s' g^{-1} \in S$



les classes de cohomologie de  $H^i(S', A)$

obtenus à partir de  $z$  par les 2

moyens évidents :  $\begin{cases} \text{restriction à } S \\ \text{restriction à } S' \text{ suivie} \\ \text{de conjugaison.} \end{cases}$

sont égales.

Quand les Sylows sont abéliens, on peut supposer  $g \in N$  (lemme de Burnside facile).

Th 4 : Il existe  $z \in H^r(G)$  qui ne donne pas à aucun sig d'ordre 2 de  $G$ .

$H^i(S)$ : polynômes homogènes de degré  $i$  en  $r$  variables.

A fabriquer: polynôme homogène en  $r$  variables  $f(x_1, \dots, x_r)$  tel que

$$f(x_1, \dots, x_r) = 1 \quad \text{pour tout}$$

$$(x_1, \dots, x_r) \in \mathbb{F}_2^r - \{0\}.$$

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 polynôme, soit  $p$ .

$$0 \rightarrow \text{Pol nég} \rightarrow \text{Pol} \rightarrow \text{Pol} / \text{Pol nég} \rightarrow 0$$

$\text{Pol nég}$  : pol. dont toutes les valeurs sur  $\mathbb{F}_2^r$  sont 0.

(Idéal des pol. nég. est engendré par les polynômes  $x_i x_j (x_i + x_j) = x_i^2 x_j + x_i x_j^2$ .)



$f \in \text{Pol} / \text{Pol}_{\text{invg}}$ . invariant par  $W$

$W$  est d'ordre impair.

Donc  $f$  est image d'un polynôme invariant.

Invariant:  $\sum_{w \in W} w(f)!$

Th 5 : L'invariant d'Arason de  $2^r q_L^0$  est

$$z_L + (-1) \dots (-1).$$

Il suffit de le voir sur  $K'$ , auquel cas

$q_L^0 = q_{L_S}$ . On est ramené au groupe  $S$

$$L_S = \bigoplus L_S^{\times}$$

$$\pi: G_K \rightarrow S = (2, \dots, 2)$$

$\pi$  correspond à  $x_1, \dots, x_r \in H^1(K)$

Invariant d'Arason cherché est

$$(-x_1) \dots (-x_r) \in H^r(K)$$

D'autre part, calculer l'image de  $t$

$$(-x_1) \dots (-x_r) = \prod (e + (x_i)) \quad e = (-1)$$

$$= e^r + \sum_{i=1}^r e^i \sum_{j_1 < \dots < j_i} (x_{j_1}) \dots (x_{j_i})$$

On peut prendre pour  $f$

$$f = \sum_{i=1}^r \sum_{j_1 < \dots < j_i} (x_{j_1})^{r-i+1} (x_{j_2}) \dots (x_{j_i})$$

$$(\text{mod } 2, x^m = x \quad m \geq 1)$$

$$\pi^*(x)^m = (-1) \dots (-1) (x) = e^{m-1}(x)$$

$$\text{car } (x)(x) = (-1)(x) = e x$$

Donc l'invariant est  $e^r + \pi^*(p)$

Th 7  $r=2$   $W$  agit par  $\zeta$

$$1 \rightarrow C_2 \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

belle base pour  $L \Leftrightarrow \pi$  réductible ds  $\tilde{G}$

D'où un  $\tilde{L}$ .



Le 2-s/g de Sylow est  $Q_8$ .

Proposition: La forme  $q_L^0$  (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

$$M = M^+ \oplus M^-$$

anti-invariants

$$\downarrow$$

$$\langle 1, \dots, 1 \rangle$$

$$\downarrow$$

$$\langle \alpha, \dots, \alpha \rangle.$$

Descente à  $K$  : dév. préservée.

Proposition

bonne base pour  $\tilde{L} \iff q_L^0 \neq \langle 1, \dots, 1 \rangle$

$\iff \alpha$  est une somme de 4 carrés

$\iff \underbrace{(-1)(-1)(\alpha)}_u = 0$  dans  $H^3(K)$ .

$$\tilde{L} \longmapsto u = (-1)(-1)(\alpha) \in H^3(K)$$

O. peut modifier  $\tilde{L}$  par  $G_K \rightarrow (\pm 1)$   
 $x \in H^1(K)$ .

Modification par  $x \in H^1(K)$  change

$$(-1)(-1)(\alpha) \text{ e. } (-1)(-1)(\alpha x)$$

O. prend  $x = \alpha$  : obstruction devient 0.  
 mod  $\boxed{4}$

Fin du cours